審査系システム　リプレイス業務及び
統合運用支援業務調達仕様書

令和５年６月
令和５年８月改訂

独立行政法人　医薬品医療機器総合機構

目次

１　調達案件の概要に関する事項

（１）　調達件名

審査系システム　リプレイス業務及び統合運用支援業務

（２）　用語の定義

表 １．１ 用語の定義

用語	概要
医薬品・医療機器 申請・審査システム（Pegasus）	医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律に定められた許認可に関する申請等を受付けて審査し、行政側の許可・承認等の業務を全国的に一括処理する基幹業務処理を行う Web システム。 医薬品等新申請・審査システムを中心とした審査関係各システムの統合、及び PMDA の業務全体の基盤となる共用 LAN システムの再構築により構築された。 厚生労働省医薬・生活衛生局の関係各課、PMDA、地方厚生局、都道府県において、医薬品等及び医療機器に係る申請等の受付、審査・調査結果の入力、許認可の施行登録、証書・通知書の発行等の業務処理と支援に用いられる。 主な機能は以下のとおり。 ・　医薬品/医療機器の製造販売許可に関する各種相談案件の管理 ・　医薬品/医療機器の製造販売許可申請受付 ・　製造販売許可申請に対する審査の進捗管理 ・　調査 (信頼性保証調査/適合性調査)案件の進捗管理　等
新 eCTD ビューアシステム （eCTD v3.2.2 ビューア）	主に医療用医薬品の製造販売承認申請の審査を行う PMDA 職員が、医療用医薬品承認申請の添付資料として企業から提出された eCTD を閲覧する際に使用する PMDA 内部に公開を限定した Web システム及び付随するクライアントツールの総称。eCTD v3.2.2 のみに対応している。 審査員は、本システムの一覧から品目を選択し、eCTD v3.2.2 ビューア機能により、eCTD を閲覧する。eCTD v3.2.2 ビューア機能の他、eCTD v3.2.2 形式の申請資料の提出受入や管理、バリデーションの実行機能などがある。また、主に申請企業が利用する eCTD v3.2.2 検証ツールや、主に外部専門委員が利用するオフラインビューア及びその出力ツールも含む。
eCTD v4 関連システム	eCTD 審査システム、eCTD v4 ビューア及び eCTD v4 検証ツールの総称。 主に医療用医薬品の製造販売承認申請の審査を行う PMDA 職員が、医療用医薬品承認申請の添付資料として企業から提出された eCTD を閲覧する際に使用する PMDA 内部に公開を限定した Web システム及び付随するクライアントツール。一部機能を除き、eCTD v3.2.2／v4 の両方に対応している。 令和４年度の承認申請品目から受付が開始されている eCTD v4 形式の申請資料の提出受入や管理、バリデーションの実行、各審査担当者の端末からの閲覧のために使用される。主に申請企業が利用する eCTD v4 検証ツールや、主に外部専門委員が利用するオフラインビューアも含む。

医薬品等 FD 申請・審査システム（旧法システム）	平成 17 年に施行された改正薬事法以前の薬事法に基づき、定められた許認可に関する申請等を受付けて審査し、行政側の許可・承認等の業務を全国的に一括処理する基幹業務処理システム。また、当該申請等を審査、調査するために開発された個別業務システムを含む総称。 改正薬事法施行前は独立して運用管理されていたが、現在は Pegasus の HW 上の仮想環境にて、稼働している。 改正薬事法施行前に提出された申請等については、改正前の法令に則り審査等を行う必要があるため、当すでに使用頻度が少なく、機能の追加・改修等は行っていないが、今後も継続的に使用される見込みである。
医療機器 WEB フォーム（DWAP）	医療機器及び体外診断薬を製造販売する企業が、インターネット経由で製造販売申請や届出を行うために利用する Web システム。 医薬品や医療機器の申請・届出には、「FD 申請ソフト」を使用して、承認申請書の電子ファイル(FD ファイル)を作成する必要があるが、本システムでは Web 上で申請内容を入力することで、適切な内容の承認申請書を作成することができる。 本システムに情報を登録するだけでは「申請行為」は行えず、窓口への書類提出が必要だが、受付後は本システムの情報が Pegasus へ連携され、PM 内で利用される。
申請電子データシステム（ゲートウェイ、GW）	新医療用医薬品の製造販売承認申請を行う企業がインターネット経由で大容量の申請資料を行政機関に提出するために開発された Web システム。現在は、医薬品に限らず FD 申請様式のオンライン届出手続き等に使用されており、今後適用範囲が拡大していく予定。なお、令和 4 年度中には原則としてすべての FD 申請様式のオンライン申請が可能となる。 申請企業が Web ブラウザを介して本システムに接続・操作することで、申請日の予告や申請に伴って添付すべき各種資料(eCTD や申請電子データ 等)を提出することができる。 本システムのサブシステムとして Pinacle 21 社の「Pinacle 21 Enterprise Edition」があり、このシステムが企業から提出された「申請電子データ」のバリデーションを実施する。 申請企業にとっては申請窓口の面を持つ一方で、PMDA 職員にとっては「申請電子データ」を管理するシステムとして扱われる。企業から提出された申請電子データを PMDA 職員が審査等の業務に活用するために、申請電子データの変換や保管を行う。なお、一部 Pegasus 画面を申請企業向けとして表示したり、機能を利用しており、本業務においては当該部分を申請電子データシステムの一部とする。
治験中不具合報告管理システム	企業から報告される医療機器の治験中に発生した不具合の情報(XML 形式)を専用ツールを利用して取り込み DB へ集積、それを PMDA 職員が検索・参照するために使用するクライアントサーバシステム。 医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律に基づき企業等より報告された治験中不具合報告等の受付及び情報管理を行う。
再生医療等製品不具合報告管理システム	「治験中不具合報告管理システム」と同じ仕組みで、再生医療等製品の治験中に発生した不具合情報の取り込み及び PMDA 職員への公開を行う。
GMP 調査関連情報集積システム (まとまるくん)	主に PMDA の品質管理部職員が使用する Microsoft Access を用いた案件管理ツール。 PMDA が行う製造所調査や GMP 適合性調査の実施履歴蓄積、調査業務計画管理、製造所情報及びリスク評価内容の管理などを本ツールで行う。 Pegasus にも同等の機能があるが、現場の業務実態に合わせツールを提供している。 本システムと Pegasus はデータ連携をしており、ツール側で更新した内容は、Pegasus に反映される。

既承認画像検索システム	承認台帳／再審査／添付資料の承認書類イメージと承認書類検索用データを蓄積・管理し、ネットワークで共有活用するクライアントサーバシステム。
審査系システム	以下のシステムの総称。 ・医薬品医療機器 申請・審査システム（Pegasus） ・申請電子データシステム（ゲートウェイ、GW） ・新 eCTD ビューアシステム（eCTD v3.2.2 ビューア） ・eCTD v4 関連システム ・医療機器 WEB 申請プラットフォーム（DWAP） ・治験中不具合管理システム ・再生医療等製品不具合報告管理システム ・医薬品等 FD 申請・審査システム（旧法システム） ・GMP 調査関連情報集積システム（まとまるくん） ・既承認画像検索システム
審査プラットフォーム（審査 PF）、審査システム共通基盤、Pegasus 基盤	審査系システムが共通して使用するハードウェア及びソフトウェアで構成するシステム基盤の総称。この基盤には、Pegasus、eCTD v3.2.2 ビューア、eCTD v4 関連システム、申請電子データシステム、DWAP、治験中不具合システム、旧法システムが存在する。
審査知識データベース	過去の審査経験・知識を的確・効率的に審査業務に活用すべく、PMDA 職員が構築したデータベースおよび参照用ツール。Microsoft Access 等を用いて作成されているが、将来的には審査系システムに統合することを検討している。
運用事業者（審査系ヘルプデスク）	審査系システムの運用保守業務（ヘルプデスク業務含む）を行う事業者。
共用 LAN システム	PMDA のイントラネットシステム。メールサーバやグループウェアサーバ、クライアント端末等で構成されている。
統合基盤	PMDA 内に存在するシステムは、共用 LAN・審査系・安全系・救済系・管理系等に分かれ、それぞれインフラ基盤を構築・運用していたが、令和 5,6 年度を目途にこれらのインフラ基盤を統合し、新しいシステムインフラ基盤を導入する予定である。この新基盤を「統合基盤」と呼び、審査系システムの各サーバやネットワークを統合基盤上で構築する。
行政機関	薬事行政業務処理を担当する厚生労働省医薬・生活衛生局の医薬品審査管理課／医療機器審査管理課／監視指導・麻薬対策課／安全対策課、7 地方厚生局薬務主管課、47 都道府県薬務主管課、PMDA を一括した呼称。

行政側担当職員	行政機関で該当する業務を担当する職員を一括して「行政側担当職員」という。これには、正職員、嘱託職員及び派遣職員が含まれる。
申請書・届書・願書（申請等）	申請者が旧薬事法または、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律に定められた許認可に関する申請・届・願（それぞれを区別しない場合、まとめて「申請等」という）を行う場合に、行政機関へ提出する書面（それぞれの書面を区別しない場合、本書においてのみ便宜的に「申請書等」という）。旧薬事法、旧薬事法施行令、旧薬事法施行規則、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律施行令、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律施行規則、厚生労働省から発出された各種通知、PMDAから発出された各種通知にその様式が定められている。
医薬品等専用ネットワーク（医薬品 NW）	PMDA 以外の行政機関（厚生労働省・厚生局・都道府県）から審査系システムにアクセスするための専用回線。当該ネットワークからのアクセスを受け入れるための設定を行う必要がある。

（３） 調達の背景

独立行政法人医薬品医療機器総合機構（以下、「PMDA」という。）では、医薬品・医療機器等の承認申請・審査関連業務を行うにあたり、次に述べるような申請・審査に関する複数のシステム（審査系システム）を稼働させている。医薬品・医療機器等の申請受付・審査業務に際しては、平成 26 年 10 月より「医薬品・医療機器 申請・審査システム（Pegasus）」を利用して、承認申請情報の参照、照会・差換え、審査等結果報告書作成等の業務を行っている。新医薬品の承認審査資料の電子データ（eCTD（電子的・コモン・テクニカル・ドキュメント））での提出を受け入れるシステムとして、平成 17 年 4 月より「新 eCTD ビューアシステム（eCTD v3.2.2 ビューア）」を、令和 4 年 4 月 1 日より「eCTD 審査システム及び eCTD v4 ビューア（eCTD v4 関連システム）」を稼働させた。また、新医薬品承認申請時に臨床試験成績の電子データ（以下、「申請電子データ」という。）を収集し、PMDA 内部での解析結果を承認審査関連業務に活用していくことを目的として、申請電子データや eCTD を含めた様々な電子ファイルをインターネットを介して提出可能とするため、「申請電子データシステム」を構築し平成 28 年 10 月から稼働させた。また申請電子データシステムにおいては、令和３年７月１日より厚生労働大臣宛て及び PMDA 理事長宛てに提出する届出書等について電子ファイルを原本とするオンライン提出が可能となり、令和３年９月１日以降は都道府県宛ての届出書等など、順次適用範囲が拡大している。

審査プラットフォームは令和７年３月末でリース期間が満了することに伴い、安定的にシステムを稼働するには新しい基盤に移行する必要がある。引き続き円滑に審査関連業務を行うためのシステム安定稼働を目的としたハードウェア及びソフトウェアの更新を行う。

また、影響範囲の広い改修等について、今回のリプレイスのタイミングで改修を行うことで効率的な改修を行えるため、このタイミングで併せて改修を行う必要があった。

今回のリプレイスにおいては、以前より検討が進められていた PMDA 情報システム基盤統合の考え方に基づき、本業務は審査プラットフォームを統合基盤に移行する作業を行う。統合基盤の概要は「閲覧資料 12 共用 LAN システム統合基盤設計資料」を参照すること。

また、PMDA では平成 30 年度より、上記の Pegasus、eCTD v3.2.2 ビューア（令和 4 年度からは eCTD v4 関連システムも対象）、申請電子データシステムの他、複数の申請・審査に関するシステムの運用支援保守業務を統合して外部に委託しており、上述のリプレイス後のシステムについて安定的に稼働および運用等を行うため、運用支援保守業務についても本業務において委託を予定している。

（４） 目的及び期待する効果

審査プラットフォームは令和７年３月末でリース期間が満了する（令和 7 年９月末まで延長予定）ことに伴い、安定的にシステムを稼働するためには新基盤に移行する必要がある。また、影響範囲の広い改修を同時に行うことにより効率的に改修を実施することができる。今回のリプレイスにおいてシステムを継続的に利用でき、また、より一層利活用しやすいシステムにすることが目的である。

さらに、リプレイス後の審査系システムについても、引き続き稼働停止することなく運用する必要があることも踏まえ、利用者に対する利便性の向上及びハードウェアの適切な管理を実施することを目的として運用支援体制を PMDA 内に確保する必要がある。また複数のシステムで機能が関連しあい、管理する情報の性質や連携を行うタイミングなどにより、不整合になるデータが発生し、また、処理誤り等によるデータの差戻し、訂正などが発生するため、円滑な運用を行うにあたっては、これらのデータ修正を関係するシステムと連携を取りながら技術的に支援する要員が必要となる。さらに、Pegasus を利用する PMDA 職員の利便性を向上させ、蓄積されたデータを有効活用するため、主に PMDA 内の利用者に対するヘルプデスクも設置する。

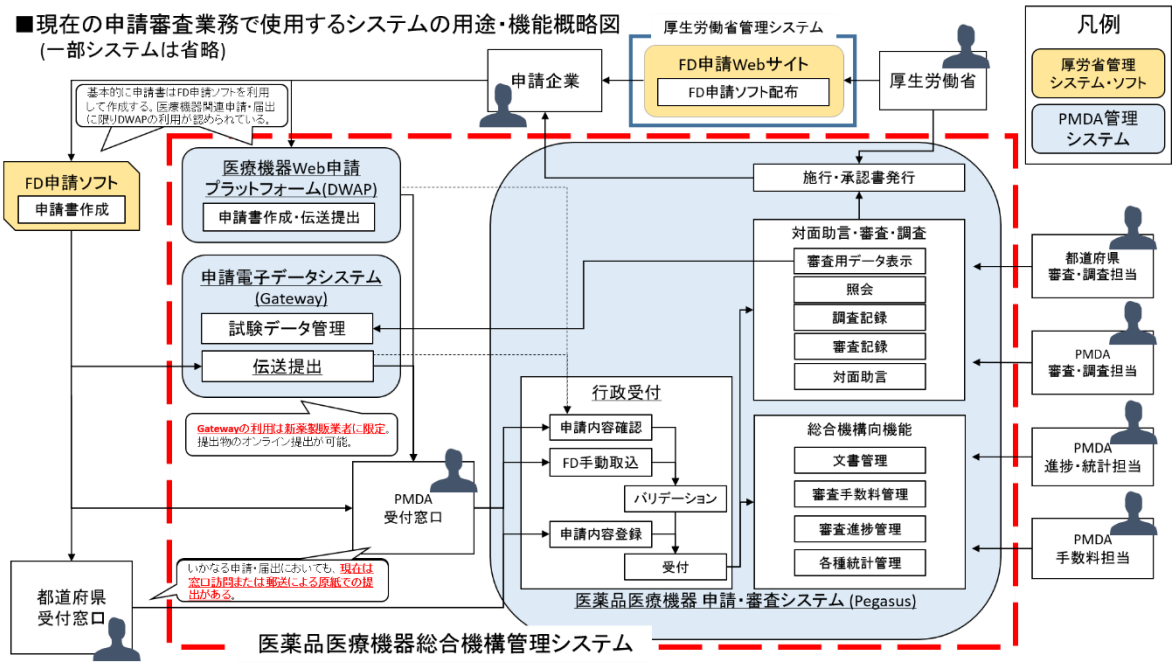
外部から要員を確保し、上記体制を整え、システムの安定的かつ効率的な稼働を維持することで、職員の遅滞の無い業務の遂行に資することを本業務の目的とする。

（５） 業務・情報システムの概要

審査プラットフォーム（以下、審査 PF という。）及び各業務システムの概要については、「１．（２）用語の定義」及び下図に示すとおりである。

システムリプレイスおよびリプレイス後の運用対象となる範囲は、Pegasus、eCTD v3.2.2 ビューア、eCTD v4 関連システム、申請電子データシステム、DWAP、治験中不具合システム（機器・再生）のアプリケーションと審査 PF となる。Pegasus のアプリケーションとし

ては、ポータル機能、ベース機能、各種業務機能に加えて、仮想環境に置かれた旧法系の機能が含まれる。申請電子データシステム及び Pegasus の外部向けポータルサイトの維持管理、後述する厚労省ヘルプデスクからの問合わせの受付（メールのみ）、対応業務及び定期報告業務も運用対象とする。EudraGMDP、日本薬局方原案進捗管理システムは審査システム共通基盤上に置かれるため、基盤運用の対象ではあるが、アプリケーションの運用は対象外となる。



また、代表的なシステムの規模及び想定利用者数等は以下の通り。

【Pegasus】

- プログラムステップ数（2022 年 9 月時点）：2652KS
- 同時ログインユーザ：内部約 228 名（内訳：PMDA170 名、厚生労働省、地方厚生局、都道府県：58 名）、外部約 100 名
- 登録利用者数：内部約 1,350 名（内訳：PMDA1,050 名、厚生労働省、地方厚生局、都道府県：300 名）、外部約 2000 名
- 申請件数（PMDA 受付）：140 件/日
- 申請件数（地方受付）：150 件/日
- 業許可：150 件/日
- 届出：4,010 件/日

【eCTD v3.2.2 ビューア／eCTD v4 関連システム】

- PMDA 内同時利用者数：約 200 名
- PMDA 内実効登録利用者数：約 1500 名

【申請電子データシステム】

- プログラムステップ数（2022 年 9 月時点）：820KS
- PMDA 内同時利用者数:全体で約 200 名（場合によっては 500 名もあり得る。）
- PMDA 内実効登録利用者数：約 1,000 名
- PMDA 外（※）実効登録利用者数：約 6,500～13,000 アカウント（利用申請者数：約 1,300 社。1 社当たり 5～10 アカウントを想定）
  ※PMDA 外は主に日本国内を想定するが、日本国外もあり得る。
- PMDA 外（行政機関のみ）同時利用者数：Pegasus と同様。
- PMDA 外（行政機関のみ）実行登録利用者数：Pegasus と同様。

なお、厚生労働省においても、令和 7 年度以降の運用支援業務の委託業者（以下、「厚労省ヘルプデスク」という。）の調達を予定している。業務内容として、厚生労働省が管理・提供する「FD 申請ソフト」、Pegasus 及び申請オンライン化に係る問合せ等の対応について、厚生労働省職員、都道府県職員及び一般ユーザ向けのヘルプデスク業務が含まれる。これらの業務内容から、厚労省ヘルプデスクと本業務受託者の間で情報連携の必要が発生する場合がある。

（６）　契約期間

契約開始日から令和 12 年 3 月 31 日までとする。

- 契約期間のうち、基盤リプレイス作業期間は契約開始日から令和 7 年 9 月 30 日までとする。
- 契約期間のうち、アプリケーション改修期間は、契約開始日から令和 7 年 6 月 30 日までとする。
- 契約期間のうち、運用支援期間は令和 7 年 7 月 1 日から令和 9 年 3 月 31 日までとする。
- 契約期間のうち､保守契約期間はハードウェア及びソフトウェア導入日から令和 12 年 3 月 31 日までとする。

（７）　SLA の締結

令和 7 年 7 月以降に実施する運用支援業務については、受託者と PMDA との間で協議の上、SLA（Service Level Agreement）を締結する。サービスレベル評価項目と要求水準については、「別紙 8　SLA（運用支援業務）」を参照すること。ただし、サービスレベル評価項目と要求水準については、必要に応じて協議の上、見直すこととする。

（８）　作業スケジュール

リプレイスに係る想定スケジュールの概要を「別紙１　審査系システムリプレイス作業スケジュール」に、運用支援業務に係る想定スケジュールの概要を「別紙９　作業スケジュール（運用支援業務）」示す。なお、詳細な実施スケジュールは受託者が検討し、PMDA と合意を得ること。

２　調達案件及び関連調達案件の調達単位、調達の方式等に関する事項

（１）　調達案件及び関連する調達案件の調達単位、調達の方式、実施時期

関連する調達案件の調達単位、調達の方式、実施時期は次の表の通りである。

表 ２．１　関連する調達案件の調達単位、調達の方式、実施時期等（既存契約）

項番	調達案件名	調達の方式	実施時期	補足
1	審査系システムリプレイス業務（ハードウェア・ソフトウェア保守）	総合評価落札方式	平成 31 年 4 月～令和 7 年 3 月	現行審査系システムを構築した業務。現在は、リースおよび保守契約が残っているが、令和 7 年 9 月末まで延長予定
2	審査系システムに係る統合運用支援業務及び統計処理業務	総合評価落札方式	令和 5 年 4 月～令和 7 年 3 月	現行システムの運用保守支援業務
3	業務システム統合基盤の構築及び保守	総合評価落札方式	令和 5 年 4 月～令和 10 年 10 月	本業務で利用するインフラ統合基盤の構築及び保守業務

表 ２．２　関連する調達案件の調達単位、調達の方式、実施時期等（契約予定）

項番	調達案件名	調達の方式	実施時期	補足
1	審査系システム改修業務(汎用化機能作成、システム統合)	未定	令和 5 年度～7 年度を予定	主に Pegasus システムのアプリケーションに対する改修業務。本業務と並行して実施するため、当該業務の成果物をリプレイス対象として考慮する必要がある。

（２）　調達案件間の入札制限

なし。

３　作業の実施内容に関する事項

（１）　作業の内容

①　設計・開発

ア　実施計画書等の作成

ア－1　受託者は、PMDA の指示に基づき、関連事業者と調整の上、以下に示す項目を記載した実施計画書の案を作成し、PMDA の承認を受けること。実施計画

書の作成に当たっては、「12 附属文書 （1）要件定義書」に記載した各事項に示す要件を参照すること。なお実施計画書を変更する必要が生じた場合は、速やかに改定計画を策定し、PMDA の承認を得て変更すること。

（実施計画書に記載する事項）

- 開発プロジェクトの概要
- 開発方針
- スケジュール
- WBS
- 役務の作業内容と完了基準
- 成果物
- 実施体制
- 要員計画
- 管理計画（コミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、構成管理、変更管理、情報セキュリティ管理）

イ　設計

イ－1　受託者は、「別紙 2 審査系システムリプレイスアプリ開発要件」「別紙 3 審査系システムリプレイスインフラ要件」に示す要件を満たすために、以下に示す基本設計作業を実施し、成果物について PMDA の承認を受けること。
なお、特にリプレイスにかかる「システム基盤方式設計」においては、審査システム基盤における全体方針が記載されるものとなるため、各設計においては「目的」も含め設計書に記載すること。
また、アプリケーション開発および改修にあたっては下記について留意し既存の設計書にかかる開発標準に合わせ設計を行うこと。

（基本設計の実施内容）

- 機能設計
- データ設計
- 画面設計
- バッチ設計
- システム基盤方式設計
- 運用設計
- 情報セキュリティ方式設計
- インターフェース設計（システム間連携）
- ファイル設計

イ－2　受託者は、基本設計書等に基づき、アプリケーションプログラムの仕様、機器等の諸元・設定内容、ソフトウェアの設定内容等を検討し、以下に示す詳細設計作業を実施し、成果物について PMDA の承認を受けること。

（詳細設計の実施内容）

- プログラム設計
- データ詳細設計
- 画面詳細設計
- 帳票詳細設計
- バッチ詳細設計
- システム基盤方式詳細設計
- 情報セキュリティ詳細設計
- インターフェース詳細設計
- 接続仕様書
- 環境定義書（パラメータシート）

イ－3　受託者は、「別紙 3 審査系システムリプレイスインフラ要件 項 13 移行要件」及び設計内容を踏まえ、移行対象、移行方式、体制と役割、移行判定基準、切り戻しの方法、リスクの識別、コンティンジェンシープラン、環境、ツール、スケジュール等を記載した移行計画の案を作成し、PMDA の確認を受けること。

イ－4　受託者は、運用設計及び保守設計を行い、情報システムの次期更改までの間に計画的に発生する作業内容、その想定される時期等を取りまとめた中長期運用・保守作業計画の案を作成し、PMDA の確認を受けること。

イ－5　受託者は、運用設計及び保守設計を行い、定常時における月次の作業内容、その想定スケジュール、障害発生時における作業内容等を取りまとめた運用計画及び保守作業計画の案を作成し、PMDA の確認を受けること。

ウ　開発・テスト

ウ－1　受託者は、開発に当たり、アプリケーションプログラムの開発又は保守を効率的に実施し、セキュリティリスクを低減したシステムを構築するため、プログラミング等のルールを定めた標準（標準コーディング規約、セキュアコーディング規約等）を定め、PMDA の確認を受けること。

また、開発に当たり、情報セキュリティ確保のためのルール遵守や成果物のセキュリティ対策の実施状況の確認方法（例えば、標準コーディング規約遵守の確認、ソースコードの脆弱性検査、現場での抜き打ち調査等についての

実施主体、手順、方法等）をセキュリティルールとして定め、PMDA の確認を受けること。

ウ－2　受託者は、「別紙 3 審査系システムリプレイスインフラ要件 項 12 テスト要件」を基に、受託者の提案書、設計書を踏まえ単体テスト、結合テスト及び総合テストについて、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載した「テスト計画書」を作成し、PMDA の承認を受けること。

ウ－3　受託者は、設計工程の成果物及び標準コーディング規約、セキュアコーディング規約、セキュリティルールに基づき、アプリケーションプログラムの開発、各種定義ファイル等の作成を行うこと。その際は、一貫した品質保証体制の下、発注者の意図しない変更や機密情報の窃取等が行われないことを保証する管理を行うこと。

ウ－4　受託者は、テスト計画書に基づき「単体テスト仕様書」、「結合テスト仕様書」を作成し、単体テスト、結合テストを実施すること。実施後速やかに「単体テスト結果報告書」、「結合テスト結果報告書」を作成し、PMDA の承認を受けること。

ウ－5　受託者は、テスト計画書に基づき「総合テスト仕様書」を作成し、総合テスト（脆弱性テスト等を含む）を実施すること。実施後速やかに「総合テスト結果報告書」及び「脆弱性検査の結果報告書」を作成し、PMDA の承認を受けること。

エ　受入テスト支援

エ－1　受託者は、「受入テスト計画書」の作成及び受入テスト実施に係る支援（テスト環境の用意、テストシナリオ及びテストデータの準備、受入テストの企画・周知並びに受入テストへの立会い等）を、受入テストに参画する関係者数を踏まえ、計画的に時間を十分に確保の上で実施すること。
また、PMDA から報告される受入テスト結果内容を取りまとめ、必要に応じて指摘事項への対応を行うこと。なお、上記の作業の実施に当たっては、「別紙 3 審査系システムリプレイスインフラ要件 項 12 テスト要件」に示す事項に留意すること。

オ　移行

オ－1　受託者は、「移行計画書」に基づき、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ等を記載した「移行テスト計画書」の案

を作成し、PMDA の承認を受けること。また、「移行テスト計画書」に基づき、移行対象データを収集・加工し、移行テストを行うこと。

オ－2　受託者は、「移行リハーサル」及び「本番移行の実施」で行われる一連の作業を対象とした「移行手順書」を作成し、PMDA の承認を受けること。なお、「移行手順書」には開発・検証した移行ツール等の、作業手順を記載し、移行ツール等の変更、更新が発生した場合は、「移行手順書」へ適宜内容を反映させること。

オ－3　受託者は、「移行計画書」、「移行手順書」及び「移行テスト計画書」に基づき、移行対象データを収集・加工し、移行リハーサルを行った上で PMDA の本番移行の開始判定を受け、本番移行を行うこと。
また、移行リハーサル、本番移行の実施において、それぞれ「移行結果報告書」を作成し、「移行計画書」に記載された判定基準に基づいた結果を PMDA に報告すること。
なお、移行計画策定から本番移行の実施作業の実施に当たっては、「別紙 3 審査系システムリプレイスインフラ要件 項 13 移行要件」に示す事項に留意すること。

カ　教育

カ－1　受託者は、「別紙 3 審査系システムリプレイスインフラ要件 項 19 教育に関する事項」に基づき、教育の対象範囲、実施方針、スケジュール、体制等を定義した上で、成果物「教育実施計画書」として取りまとめ、PMDA の承認を受けること。

カ－2　受託者は、「別紙 3 審査系システムリプレイスインフラ要件 項 19 教育に関する事項」に基づき、必要となる資料を作成すること。

カ－3　受託者は、「別紙 3 審査系システムリプレイスインフラ要件 項 19 教育に関する事項」及び「教育実施計画書」に基づき、教育を実施し、実施結果の報告を行うこと。

② 運用支援

ア　運用業務

「別紙 10　業務要件（運用支援業務）」に基づき、システム運用を行うこと。
作業は、基本的に「運用計画書（※1）」、「運用手順書（※1）」、「プロジェクト実施計画書（※2）」に基づき実施し、必要に応じて PMDA と協議し実施すること。また、必要に応じて PMDA と協議し、ドキュメントの作成・改版等を行うこと。

※1　PMDA より提示される。

※2　運用計画書、運用手順書・保守計画書・保守手順書等に基づき、具体的な実行計画をたてて作成すること。

a　サービスレベル管理

b　稼働統計確認集計

c　計画停止

d　バックアップ／リストア

e　セキュリティ対策

f　運用監視

g　障害対応／セキュリティインシデント対応（障害原因調査を含む）

h　作業依頼対応

i　アクセス管理

j　問合せ対応

k　情報提供

l　変更管理

m　構成管理

n　時刻同期管理

o　ログ抽出

p　運用サービスレポート

q　証明書類の更新

r　統計処理

s　情報資産棚卸しおよびリスク評価支援対応

t　拠出金徴収管理システムにおける期末期首処理の支援

u　その他の作業

イ　保守業務

「別紙 10 業務要件（運用支援業務）」に基づき、システム保守作業を行うこと。

作業は、基本的に「保守計画書（※1）」、「保守手順書（※1）」、「プロジェクト実施計画書（※2）」に基づき実施し、必要に応じて PMDA と協議し実施すること。また、必要に応じて PMDA と協議し、ドキュメントの作成・改版等を行うこと。なお、システムごとに対応する内容が異なるため、詳細は「別紙 11 その他

の要件（運用支援業務）」を参照のこと。

※1　PMDA より提示される。

※2　運用計画書、運用手順書・保守計画書・保守手順書等に基づき、受託者が具体的な実行計画をたてて作成すること。

a　アプリケーション保守

b　アップデート

c　試験データバリデーションルールの変更に伴うシステム変更

ウ　システム改修、その他業務

上記「運用業務」「保守業務」に含まれないシステム改修及び対応を行う。詳細は、「別紙 10 業務要件（運用支援業務）」を参照すること。

a　審査知識データベース維持・管理業務

エ　報告業務

「別紙 10 業務要件（運用支援業務）」の「運用サービスレポート」で説明する報告業務を行う。

エ－1　日々の運用業務の記録と作業月報の作成を行い、定期的に提出すること。

エ－2　現有構成の中での監視にてシステムやデータベースの障害等が予見された場合には、当該事象を知った後、速やかに PMDA に報告し、その対応については PMDA と協議すること。

エ－3　月例報告会の開催

PMDA と協議の上、開催方法・日程等を調整し月例報告会を開催すること。開催頻度は原則として月１回を予定する。ただし、必要に応じて臨時に報告会を開催することがある。報告書に記載する内容は以下を含むものとする。

- PMDA 及び申請企業からの問い合わせ状況・対応の報告
- システム稼動状況やサービスレベルの遵守状況の報告
- 障害発生状況・対応（運用による回避策を含む）の報告
- 保守改修やドキュメント作成業務の進行状況
- 本業務従事者の情報（氏名、業務開始日、常勤／非常勤の別、加入申請日　等）の報告
- PMDA が管理するエリアから物理的記録媒体にて持ち出した情報の管理状況（対象物と現在の状態、事前申請有無、取り扱い終了の報告有無）の報告
- その他（利用者への障害や回避方法の周知を含む）

エ－4　その他運用支援に関する報告

受託者は、運用業務を実施するにあたって明らかになった、システムの見直しが必要と考えられる事項を運用支援報告書としてとりまとめ、年度末に提出すること。ただし、業務上支障を生ずる問題やセキュリティ上のリスク等については、報告自体は影響範囲等明確にしたうえで判明次第早急に行うこと。都度報告が必要と判断される際は、報告書として体裁等整える必要はない。なお、特に各システムで使用しているソフトウェア等のサポート期限が満了することによる影響は大きいため、十分に留意すること。

また、必要に応じて、運用作業計画、運用手順書、保守作業計画、保守作業手順、運用実施要領等に対する改善案があれば報告すること。

オ　支援業務時間

支援業務を行う日は、本書で別途定められている業務の他は、行政機関の休日（「行政機関の休日に関する法律」（昭和 63 年法律第 91 号）第 1 条第 1 項に掲げる日をいう。）を除く日とする。

また、支援業務を行う時間については、原則、支援業務を行う日の 9 時 30 分から 18 時 00 分までとする。PMDA の始業時間等が時差出勤等により変更になる場合は、支援業務を行う時間帯を変更（30～60 分程度を想定）する可能性がある事に留意すること。（ヘルプデスク業務に支障をきたさないように調整した上で、1 時間の休憩時間をとる。）

ただし、本書で別途定めるものの他、緊急作業及び本業務を実施するために必要な作業がある場合は、この限りではない。

カ　引継ぎ

カ－1　運用保守業務対象システムの更改時

受託者は、PMDA が運用保守業務対象システムの更改を行う際には、次期の情報システムにおける要件定義支援事業者及び設計・開発事業者等に対し、現在のシステムの状況、機能・構成、残存課題等に関する情報提供及び質疑応答等の協力を行うこと。

カ－2　現行運用事業者からの引継ぎ

受託者は、現行運用事業者から運用に必要な事項の引継ぎとして、運用監視作業エリアの引継、サービスデスクの引継、システム資源及びデータの引継を受け、現行事業者から提供される資料（運用作業の計画書や報告書、運用設計書及び運用手順書等の一覧）を基に自主的に業務習熟を行うこと。現行運用事業者からの引継作業は受託者の負担と責任において実施すること。

カ－3　次期運用事業者への引継ぎ

受託者は、本業務に係る契約期間終了後、受託者と異なる事業者が本情報システムの運用業務を受託した場合には、次期運用事業者に対し、作業経緯、残存課題等下記項目についての引継ぎを行うこと。

A) 問合せ、障害等の対応及び管理に関する手法・手順
B) システム運用マニュアル、運用業務マニュアル
C) 仕掛中の項目一覧及びその進捗状況
D) 過去の問合せ、障害等の実績及びその対応方法
E) バックログ・未対応作業一覧及びその対応(案)
F) その他業務を引継ぐ上で必要と思われる事項

③　ハードウェア及びソフトウェア保守

ア　中長期運用・保守作業計画の確定支援

ア－1　受託者は、PMDA が中長期運用・保守作業計画を確定するに当たり、情報システムの構成やライフサイクルを通じた運用業務及び保守作業の内容について、計画案の妥当性の確認、情報提供等の支援を行うこと。

イ　保守作業計画及び保守実施要領の作成支援

イ－1　受託者は、PMDA が保守作業計画及び保守実施要領を作成するに当たり、具体的な作業内容や実施時間、実施サイクル等に関する資料作成等の支援を行うこと。

ウ　定常時対応

ウ－1　受託者は、「別紙 3　審査系システムリプレイスインフラ要件」の保守要件に示す定常時保守業務（不具合受付等）を行うこと。具体的な実施内容・手順は PMDA が定める保守作業計画に基づいて行うこと。

エ　障害発生時対応

エ－1　受託者は、情報システムの障害発生時（又は発生が見込まれる時）には、PMDA 又は運用事業者からの連絡を受け、「別紙 3　審査系システムリプレイスインフラ要件」の保守要件に示す障害発生時保守業務（原因調査、応急措置、報告等）を行うこと。障害には、情報セキュリティインシデントを含めるものとする。具体的な実施内容・手順は PMDA が定める「インシデント管理標準手順書」に基づいて行うこと。

エ－2　受託者は、情報システムの障害に関して事象の分析（発生原因、影響度、過去の発生実績、再発可能性等）を行い、同様の事象が将来にわたって発生す

る可能性がある場合には、恒久的な対応策を提案及び対応策の実施をすること。

エ－3　受託者は、大規模災害等の発災時には、PMDA の指示を受けて、必要な対応を実施すること。

オ　その他

オ－1　受託者は、PMDA が本システムの更改を行う際には、次期の情報システムにおける PMDA 及び設計・開発事業者等に対し、作業経緯、残存課題等に関する情報提供及び質疑応答等の協力を行うこと。

④　現行システム機器の撤去および返却、廃棄

ア　受託者は、本業務の本番移行作業完了後、現行システム機器が設置されているデータセンタにて、機器の撤去と返却、廃棄を PMDA の求めに応じて、受託者の責任と負担において実施すること。詳細を「別紙 3　審査系システムリプレイスインフラ要件」に示す。廃棄対象については、「閲覧資料 11 前回リプレイス（令和元年度）審査系システム共通基盤設計資料」を参照のこと。

（２）　システム資産簿登録に係る作業

①　PMDA においては、システムのインベントリ情報を一元管理するシステム資産簿を作成している。受託者は、本システムで利用する機器、ソフトウェア、ネットワーク等の構成情報を PMDA へ報告し、一元管理するシステム資産簿の管理情報について常に最新の状態を保つこと。なお、以下に示す事項以外に管理が必要と考えられる事項があれば PMDA と協議の上、合わせて管理すること。

②　受託者は、PMDA が指定する以下のシステム資産簿登録用シートを、運用実施要領において定める時期に提出すること。

ア　ハードウェア管理台帳（ハードウェア名称、システムモデル、シリアル番号、サポート内容・期間等）

イ　ソフトウェア管理台帳（ソフトウェア名称、エディション・バージョン、ソフトウェアの搭載機器、サポート内容・期間等）

ウ　ライセンス管理台帳（ソフトウェア名称、エディション・バージョン、ライセンス番号（シリアル番号）、提供形態、有効期限、保有ライセンス数等）

エ　その他 PMDA が指定する項目

③　受託者は、本システムを構成する機器・ソフトウェアの変更、業務アプリケーション

の変更、仕様書、設計書等の本システムにかかる各種ドキュメントの変更について、変更理由、変更内容、影響範囲、対応状況、責任者、対応者等と記録し、一元管理を行うこと。

（３）　成果物の範囲、納品期日等

① 成果物

作業工程別の納入成果物を表 ３.１、表 ３.２、表 ３.３に示す。ただし、納入成果物の構成、詳細については、受託後、PMDA と協議し取り決めること。なお、各業務に含まれる作業範囲は、下記に該当するものとする。

リプレイス業務・・・３－（１）－①

改修業務・・・・・・３－（１）－②－イ－a, c

運用業務・・・・・・３－（１）－②の上記以外、３－（１）－③

表 ３.１　主にリプレイス業務に伴う成果物　工程と成果物

項番	工程	納入成果物	納入期日	納品に関する注意事項
1	計画	・実施計画書（開発プロジェクト概要、開発方針、スケジュール、WBS、作業内容と完了基準、成果物、実施体制、要員計画、管理計画、情報セキュリティ管理計画）	契約締結日から 2 週間以内	
2	基本設計（業務 AP）	・基本設計書	詳細設計（業務 AP）開始前まで	
3	基本設計（基盤）	・基本設計書 ・統合基盤ヒアリングシート	詳細設計（基盤）開始前まで	
4	詳細設計（業務 AP）	・詳細設計書	製造開始前まで	
5	詳細設計（基盤）	・詳細設計書（パラメータシート）	基盤構築開始前まで	
6	導入	・導入計画書 ・導入手順書 ・導入作業結果報告書 ・ソフトウェア製品 ・ハードウェア製品	導入開始前まで	
7	単体テスト（業務 AP）	・単体テスト計画書 ・単体テスト結果報告書 ・単体テスト結果エビデンス ・テストデータ	結合テスト（業務 AP）開始前まで	
8	結合テスト（業務 AP）	・結合テスト計画書 ・結合テスト結果報告書 ・結合テスト結果エビデンス	総合テスト（業務 AP）開始前まで	

項番	工程	納入成果物	納入期日	納品に関する注意事項
		・テストデータ		
9	総合テスト（業務AP）	・総合テスト計画書 ・総合テスト結果報告書 ・総合テスト結果エビデンス ・テストデータ	受入テスト開始前まで	
10	単体テスト（基盤）	・単体テスト計画書 ・単体テスト結果報告書 ・単体テスト結果エビデンス	結合テスト（基盤）開始前まで	
11	結合テスト（基盤）	・結合テスト計画書 ・結合テスト結果報告書 ・結合テスト結果エビデンス	総合テスト（基盤）開始前まで	
12	総合テスト（基盤）	・総合テスト計画書 ・総合テスト結果報告書 ・総合テスト結果エビデンス	受入テスト開始前まで	
13	脆弱性検査結果報告書	脆弱性検査結果を報告する文書を指す。	受入テスト開始前まで	
14	移行	・移行計画書 ・移行手順書 ・移行プログラム及びツール ・移行リハーサル実施要領 ・移行リハーサル結果報告書 ・本番移行実施要領 ・移行実施結果報告書	移行開始前まで	
15	教育	・教育計画書 ・教育用資料 ・教育作業結果報告書等	教育開始前まで	
16	廃棄	・廃棄結果証明書	令和7年9月19日（※必要に応じて随時提出）	
17	保守	・保守計画書 ・保守手順書 ・保守引継計画書 ・保守引継完了報告書	令和7年9月19日 ※必要に応じて随時提出）	（
18	その他	・打合せ資料 ・議事録 ・機密情報受理管理簿 ・撤去機器一覧 ・データ消去証明書 ・瑕疵担保責任対応に係る保有情報の一覧 ・プロジェクト完了報告書 ・保守報告書	令和7年9月19日（※必要に応じて随時提出）	

表 3．2　主に運用業務に伴う成果物 工程と成果物一覧

項番	工程	納入成果物 (注 1)	納入期日	納品に関する注意事項
1	計画	・プロジェクト実施計画書 （プロジェクトスコープ、体制表、作業分担、スケジュール、文書管理要領、セキュリティ管理要領、品質管理要領、変更管理要領、WBS 等） ・情報セキュリティ管理計画書(注 2)	契約締結日から 2 週間以内	
2	運用	・運用計画書（改版） ・運用手順書（追加・改版） ・操作手順書（追加・改版） ・運用支援要員業務マニュアル ・その他システム関連ドキュメント（パッチの適用や障害対応、軽微な改修等により追加・変更した設計書、操作マニュアル等を必要に応じて提出すること） ・プログラム・ツール等	令和 9 年 3 月 31 日 （※PMDA が求めた際は必要に応じて随時提出すること）	
3	その他	・作業月報 ・月例報告資料 ・稼働状況報告書 ・打合せ資料 ・議事録 ・障害等作業記録 ・運用支援報告書	月報は毎月末日、 その他は令和 9 年 3 月 31 日 （※必要に応じて随時提出）	

表 3．3　主に保守改修業務に伴う成果物 工程と成果物

項番	工程	納入成果物 (注 1)	納入期日	納品に関する注意事項
1	計画	・プロジェクト実施計画書 （プロジェクトスコープ、体制表、作業分担、スケジュール、文書管理要領、セキュリティ管理要領、品質管理要領、変更管理要領、WBS 等） ・情報セキュリティ管理計画書(注 2)	契約締結日から 2 週間以内	表 3.1 のプロジェクト実施計画書と同一内容可
2	改修	・操作手順書（追加・改版） ・保守計画書（改版） ・保守手順書（追加・改版） ・運用支援要員業務マニュアル ・その他システム関連ドキュメント（パッチの適用や障害対応、軽微な改修等により追加・変更した設計書、操作マニュアル等を必要に応じて提出すること） ・プログラム・ツール等 ・使用した開発用データ	令和 9 年 3 月 31 日 （※PMDA が求めた際は必要に応じて随時提出すること）	
3	その他	・打合せ資料 ・議事録 ・障害等作業記録	令和 9 年 3 月 31 日 （※必要に応じて随時提出）	

注１　納入成果物の作成にあたっては、SLCP-JCF2013（共通フレーム 2013）を参考とすること。

注２　情報セキュリティ管理計画書には、ＩＳＭＳ等認証取得、情報管理に関するルール（社内規程明示等）、情報管理体制、情報セキュリティインシデント対処方法、PMDA 情報の取扱い（目的外使用・意図しない変更を防止する方法を含む）、メンバーのスキル・資格・国籍等、自主点検の実施、業務環境のセキュリティ、レポート体制、再委託による履行保証措置、緊急連絡方法、教育・研修の実施等を記載

② 納品方法

表 ３.１の納入成果物を含む全ての納入成果物を各納入期日までに納品すること。なお、納入成果物については、以下の条件を満たすこと。

ア　文書を外部電磁的記録媒体（CD-R, DVD-R, BD-R 等)により日本語で提供すること。なお、紙媒体による提供は不要である。

イ　磁気媒体等に保存するファイルの形式は、PDF 形式及び Microsoft 365 で扱える形式とする。ただし、PMDA が別に形式を定めて提出を求めた場合は、この限りではない。

ウ　磁気媒体については二部ずつ用意すること。

エ　一般に市販されているツール、パッケージ類の使用は PMDA と協議の上、必要であれば使用を認めることとするが、特定ベンダーに依存する（著作権、著作者人格権を有する）ツール等は極力使用しないこと。

オ　本業務で使用した開発ツール等の使用開始後５年間分のライセンス及びメディアを納入すること。

カ　本業務を実施する上で必要となる一切の機器物品等は、受託者の責任で手配するとともに、費用を負担すること。

キ　各工程の中間成果物も含め、本業務に係る全ての資料を納品すること。

③ 納品場所

独立行政法人　医薬品医療機器総合機構　審査マネジメント部

４　満たすべき要件に関する事項

リプレイス業務の実施にあたっては、審査系システムの設計書等及び以下を参照し、本業務に求められる各要件を満たすこと。要件に関するその他資料は「12　附属資料　(2) 事業者が閲覧できる資料一覧」のとおりである。受託者は、これらの資料を横断的に参照して、各要件を満たすように作業を実施すること。

- 別紙２　審査系システムリプレイスアプリ開発要件

・　別紙 3　審査系システムリプレイスインフラ要件
・　別紙 6　審査系システム構成要件

令和 7 年 7 月以降の運用支援業務の実施にあたっては、以下に記載の各要件を満たすこと。

・　別紙 8　SLA（運用支援業務）
・　別紙 10　業務要件（運用支援業務）
・　別紙 11　その他の要件（運用支援業務）
・　別紙 12　システム運用管理基準
・　別紙 13　情報セキュリティ対策の運用要件
・　閲覧資料 3　セキュリティ管理要件書(ひな型)

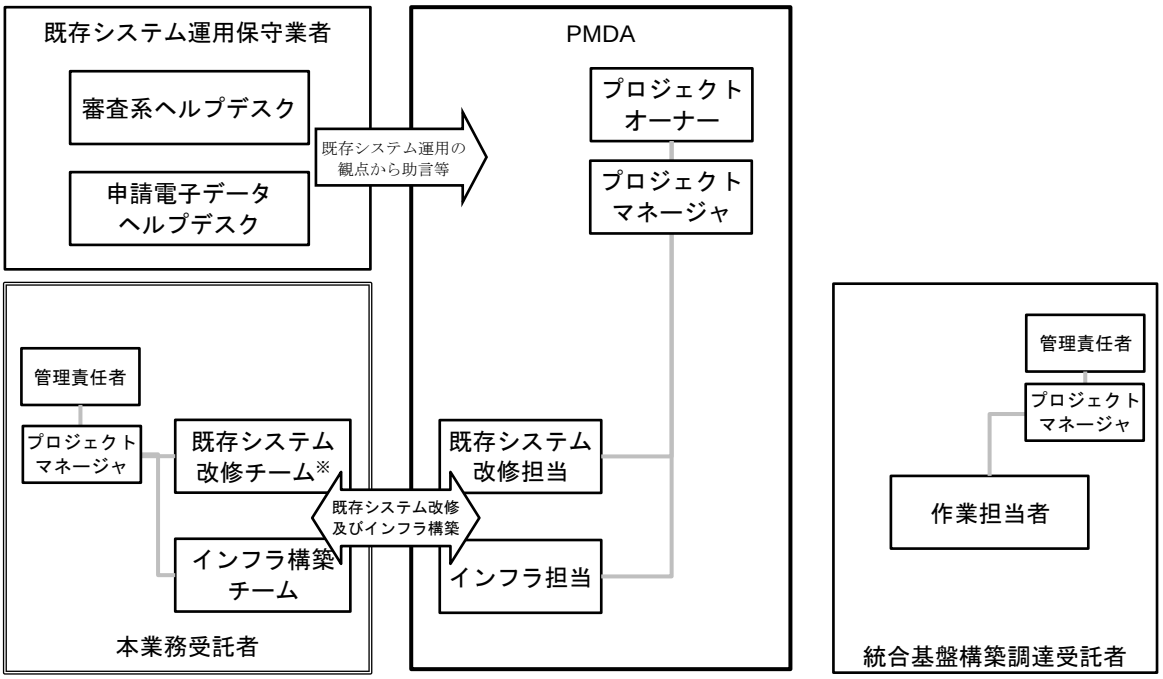
５　作業の実施体制・方法に関する事項

（１）　作業実施体制

受託者は、本業務に係る要員の役割分担、責任分担、体制図等を実施計画書の一部として作成し、PMDA に報告するとともに、承認を得ること。また、受託者は、必要な要員の調達を遅滞なく実施し、要員を確定すること。

なお、令和 7 年 7 月以降の運用支援業務における SLA を満たすために PMDA 内に常勤する必要があると考えられるヘルプデスクの要員数として、PMDA では 15 名程度を想定している。なお最大 17 名程度の座席は確保できるため、過渡期や受託者内部での引継ぎ等で増員する必要がある場合は PMDA と協議の上増員すること。また、社会情勢等で PMDA から常勤者の削減を要求する場合があるが、その場合における SLA の取り扱いなどについては協議の上対応すること。なお、保守作業等で PMDA に常勤しない担当者数は特に制限しない。

①　プロジェクトの推進体制及び本件受託者に求める作業実施体制は「図 5-1」のとおりである。なお、受託者内のチーム編成については想定であり、受託者決定後に協議の上、見直しを行うこと。また、受託者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。



※既存システム改修チームは令和７年７月以降も継続する

図　５．１　プロジェクト実施体制（～令和７年６月）

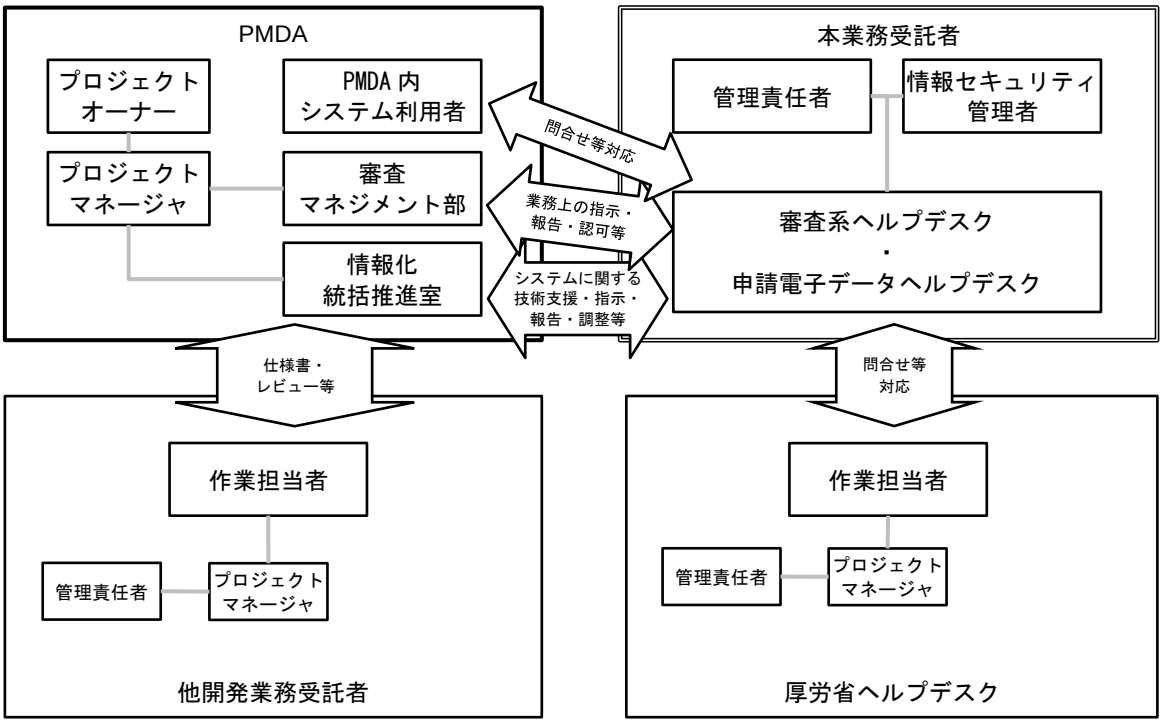


図　５．２　プロジェクト実施体制（令和７年７月以降）

②　システム設計・導入等を複数業者が連携（再委託を含めて）して実施する等の場合は、参画する各業者の役割分担等を明示すること。

③　本業務の実施に当たり、PMDA の意図しない変更が行われないことを保証する管理が、

一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。

④ 本情報システムにPMDAの意図しない変更が行われるなどの不正が見つかった時(不正が行われていると疑わしい時も含む）に、追跡調査や立入検査等、PMDAと受託者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

⑤ 当該管理体制を確認する際の参照情報として、資本関係・役員等の情報、本業務の実施場所、本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供を行うこと。具体的な情報提供内容についてはPMDAと協議の上、決定するものとする。

⑥ 受託者は、インシデント発生時などの連絡体制図をPMDAと協議の上定めること。

⑦ 令和7年7月以降の運用支援業務において、当初想定した体制ではSLAの順守が困難となった場合は、運用に影響を与えないよう、受託者の負担と責任で要員の交代や増員などの措置を講じ、可能な限り速やかにSLAの順守状況を改善すること。また、要員数や各要員の稼働状況を月次にて報告すること。

（２） 作業要員に求める資格等の要件

① 本プロジェクト全体の管理を行う責任者は、特定非営利活動法人 日本プロジェクトマネジメント協会の「プロジェクトマネジメント・スペシャリスト（PMS）」、PMI（Project Management Institute)の「PMP」資格、独立行政法人情報処理推進機構（IPA）の「プロジェクトマネージャ」資格のいずれかを取得していること。

② 設計・開発に携わるリーダは、医薬品等の申請・審査業務を理解しており、本業務システムの設計にあたり、PMDAに逐次業務の説明を求めることなく担当者とスムーズな会話ができる知識を有していること。

③ 基盤構築に携わるリーダは、独立行政法人情報処理推進機構（IPA）の「ネットワークスペシャリスト」、「データベーススペシャリスト」、「情報処理安全確保支援士」のいずれかに該当すること。もしくは上記資格保有者等と同様の能力を有することが経歴等において明らかであること。

④ 運用支援業務に携わるリーダは、特定非営利活動法人 日本プロジェクトマネジメント協会の「プロジェクトマネジメント・スペシャリスト（PMS）」、PMI（Project Management Institute）の「PMP」資格、独立行政法人情報処理推進機構（IPA）の「プロジェクトマネージャ」資格のいずれかを取得していること。

⑤ 運用支援業務に携わるメンバーの1人は、独立行政法人情報処理推進機構（IPA）の「情報セキュリティスペシャリスト」もしくは「情報処理安全確保支援士」のいずれかの資格を取得していること。

⑥ 運用支援業務に携わるメンバーの1人は、Microsoft Access VBA（Microsoft Access内で有効なSQLやDAO、FSOを含む）を用いたプログラムを、自身の設計により作

成し、継続的に管理運用（改修を含む）した経験及びそのための能力を有すること。

⑦ 運用支援業務に携わるメンバーは、医薬品等の申請・審査業務を理解しており、本業務システムの設計にあたり、PMDA に逐次業務の説明を求めることなく担当者とスムーズな会話ができる知識を有していること。

（３） 作業場所

① 本業務の作業場所（サーバ設置場所等を含む）は、（再委託も含めて）PMDA 内、又は日本国内で PMDA の承認した場所で作業すること。

② 本業務で用いるサーバ、データ等は日本国外に持ち出さないこと。

③ PMDA 内での作業においては、必要な規定の手続を実施し承認を得ること。

④ なお、必要に応じて PMDA 職員は現地確認を実施できることとする。

（４） 作業の管理に関する要領

① 受託者は、PMDA が承認した業務実施要項に基づき、本業務に係るコミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

② 受託者は、PMDA の指示に従って運用支援業務に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

③ PMDA が管理するエリアからの情報の持ち出しは許可しない。持ち出しが必要な場合は事前に PMDA に対し、持ち出し目的、対象情報の範囲、情報利用端末、情報の利用者等に関し申請を行うこと。また受託者は、持ち出した情報を台帳等により管理し、USB メモリ等の物理的記録媒体により持ち出した情報の有無及び管理状況（対象物と現在の状態、事前申請有無、取り扱い終了の報告有無 等）を月次にて報告すること。さらに受託者は、持ち出した情報は使用後に確実に消去し、そのエビデンスを提出すること。

６ 作業の実施に当たっての遵守事項

（１） 基本事項

受託者は、次に掲げる事項を遵守すること。

① 本業務の遂行に当たり、業務の継続を第一に考え、善良な管理者の注意義務をもって誠実に行うこと。

② 本業務に従事する要員は、PMDA と日本語により円滑なコミュニケーションを行う能力と意思を有していること。

③ 本業務の履行場所を他の目的のために使用しないこと。

④ 本業務に従事する要員は、履行場所での所定の名札の着用等、従事に関する所定の規則に従うこと。
⑤ 要員の資質、規律保持、風紀及び衛生・健康に関すること等の人事管理並びに要員の責めに起因して発生した火災・盗難等不祥事が発生した場合の一切の責任を負うこと。
⑥ 受託者は、本業務の履行に際し、PMDA からの質問、検査及び資料の提示等の指示に応じること。また、修正及び改善要求があった場合には、別途協議の場を設けて対応すること。
⑦ 次回の本業務調達に向けた現状調査、PMDA が依頼する技術的支援に対する回答、助言を行うこと。
⑧ 本業務においては、業務終了後の運用等を、受託者によらずこれを行うことが可能となるよう詳細にドキュメント類の整備を行うこと。

（２） 機密保持、資料の取扱い

本業務を実施する上で必要とされる機密保持に係る条件は、以下のとおり。

① 受託者は、受託業務の実施の過程で PMDA が開示した情報（公知の情報を除く。以下同じ。）、他の受託者が提示した情報及び受託者が作成した情報を、本受託業務の目的以外に使用又は第三者に開示若しくは漏洩してはならないものとし、そのために必要な措置を講ずること。
② 受託者は、本受託業務を実施するにあたり、PMDA から入手した資料等については管理簿等により適切に管理し、かつ、以下の事項に従うこと。
- 複製しないこと。
- 用務に必要がなくなり次第、速やかに PMDA に返却又は消去すること。
- 受託業務完了後、上記①に記載される情報を削除又は返却し、受託者において該当情報を保持しないことを誓約する旨の書類を PMDA に提出すること。

③ 応札希望者についても上記①及び②に準ずること。
④ 「独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程」の第 52 条に従うこと。
⑤ 「秘密保持等に関する誓約書」を別途提出し、これを遵守しなければならない。
⑥ 機密保持の期間は、当該情報が公知の情報になるまでの期間とする。

（３） 遵守する法令等

本業務を実施するにあたっての遵守事項は、以下のとおり。

① 受託者は、最新の「政府機関のサイバーセキュリティ対策のための統一基準」、「府省庁対策基準策定のためのガイドライン」、「医療情報システムの安全管理に関するガイドライン」及び「独立行政法人　医薬品医療機器総合機構サイバーセキュリティ

ポリシー」（以下、「セキュリティポリシー」という。）に遵守すること。セキュリティポリシーは非公表であるが、「政府機関のサイバーセキュリティ対策のための統一基準群」に準拠しているので、必要に応じ参照すること。セキュリティポリシーの開示については、契約締結後、受託者が担当職員に「秘密保持等に関する誓約書」を提出した際に開示する。

② PMDA へ提示する電子ファイルは事前にウイルスチェック等を行い、悪意のあるソフトウェア等が混入していないことを確認すること。

③ 民法、刑法、著作権法、不正アクセス禁止法、個人情報保護法等の関連法規を遵守することはもとより、下記の PMDA 内規程を遵守すること。

- 独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程
- 独立行政法人 医薬品医療機器総合機構 個人情報管理規程

④ 受託者は、本業務において取り扱う情報の漏洩、改ざん、滅失等が発生することを防止する観点から、情報の適正な保護・管理対策を実施するとともに、これらの実施状況について、PMDA が定期又は不定期の検査を行う場合においてこれに応じること。万一、情報の漏洩、改ざん、滅失等が発生した場合に実施すべき事項及び手順等を明確にするとともに、事前に PMDA に提出すること。また、そのような事態が発生した場合は、PMDA に報告するとともに、当該手順等に基づき可及的速やかに修復すること。

7　成果物の取扱いに関する事項

（１）　知的財産権の帰属

知的財産の帰属は、以下のとおり。

① 本件に係り作成・変更・更新されるドキュメント類及びプログラムの著作権（著作権法第 21 条から第 28 条に定めるすべての権利を含む。）は、受託者が本件のシステム導入の従前より権利を保有していた等の明確な理由により、あらかじめ書面にて権利譲渡不可能と示されたもの以外、PMDA が所有する等現有資産を移行等して発生した権利を含めてすべて PMDA に帰属するものとする。

② 本件に係り発生した権利については、受託者は著作者人格権（著作権法第 18 条から第 20 条までに規定する権利をいう。）を行使しないものとする。

③ 本件に係り発生した権利については、今後、二次的著作物が作成された場合等であっても、受託者は原著作物の著作権者としての権利を行使しないものとする。

④ 本件に係り作成・変更・修正されるドキュメント類及びプログラム等に第三者が権利を有する著作物が含まれる場合、受託者は当該著作物の使用に必要な費用負担や使用許諾契約に係る一切の手続きを行うこと。この場合は事前に PMDA に報告し、承認を得ること。

⑤ 本件に係り第三者との間に著作権に係る権利侵害の紛争が生じた場合には、当該紛争

の原因が専ら PMDA の責めに帰す場合を除き、受託者の責任、負担において一切を処理すること。この場合、PMDA は係る紛争の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者にゆだねる等の協力措置を講ずる。
なお、受託者の著作又は一般に公開されている著作について、引用する場合は出典を明示するとともに、受託者の責任において著作者等の承認を得るものとし、PMDA に提出する際は、その旨併せて報告するものとする。

（２） 契約不適合責任

① 受託者は本業務の成果物に対する契約不適合責任を負うものとする。本業務の最終検収後において、委託業務の納入成果物に関して仕様書と異なる、または契約目的に照らして通常期待される条件を満たしていない等、本システムの安定稼動等に関わる契約不適合の疑いが生じた場合であって、PMDA が下記で定める期間内に調査を求めた場合は、受託者は速やかに契約不適合の疑いに関して調査し回答すること。調査の結果、納入成果物に関して契約不適合等が認められた場合には、受託者の責任及び負担において速やかに修正を行うこと。なお、修正を実施する場合においては、修正方法等について、事前に PMDA の承認を得てから着手すると共に、修正結果等について、PMDA の承認を受けること。

② 受託者は、契約不適合責任を果たす上で必要な情報を整理し、その一覧を PMDA に提出すること。契約不適合責任の期間が終了するまで、それら情報が漏洩しないように、ISO/IEC27001 認証（国際標準規格）又は JISQ27001 認証（日本産業標準規格）に従い、また個人情報を取り扱う場合には JISQ15001（日本工業規格）に従い、厳重に管理をすること。また、契約不適合責任の期間が終了した後は、速やかにそれら情報をデータ復元ソフトウェア等を利用してもデータが復元されないように完全に消去すること。データ消去作業終了後、受託者は消去完了を明記した証明書を作業ログとともに PMDA に対して提出すること。なお、データ消去作業に必要な機器等については、受託者の負担で用意すること。

③ 契約不適合責任の期間は別途契約書で定めるものとする。

（３） 検収

納入成果物については、適宜、PMDA に進捗状況の報告を行うとともに、レビューを受けること。最終的な納入成果物については、「3（3）①成果物」に記載のすべてが揃っていること及びレビュー後の改訂事項等が反映されていることを、PMDA が確認し、これらが確認され次第、検収終了とする。

なお、以下についても遵守すること。

① 検査の結果、納入成果物の全部又は一部に不合格品を生じた場合には、受託者は直ちに引き取り、必要な修復を行った後、PMDA の承認を得て指定した日時までに修正が

反映されたすべての納入成果物を納入すること。

② 「納入成果物」に規定されたもの以外にも、必要に応じて提出を求める場合があるので、作成資料等を常に管理し、最新状態に保っておくこと。

③ PMDA の品質管理担当者が検査を行った結果、不適切と判断した場合は、品質管理担当者の指示に従い対応を行うこと。

8 入札参加資格に関する事項

（1） 入札参加要件

応札希望者は、以下の条件を満たしていること。

① 導入責任部署は ISO9001 又は CMMI レベル 3 以上の認定を取得していること。

② ISO/IEC27001 認証（国際標準）又は JISQ27001 認証（日本工業標準）のいずれかを取得していること。

③ プライバシーマーク付与認定を取得していること。

④ PMDA にて現行関連システムの設計書等を閲覧し、内容を十分理解していること。

⑤ 中央省庁において、本業務と同等規模以上の業務実績を 5 件以上有すること。

⑥ 応札時には、導入作業毎に十分に細分化された工数、概算スケジュールを含む見積り根拠資料の即時提出が可能であること。なお、応札後に PMDA が見積り根拠資料の提出を求めた際、即時に提出されなかった場合には、契約を締結しないことがある。

（2） 入札制限

情報システムの調達の公平性を確保するために、以下に示す事業者は本調達に参加できない。

① PMDA の CIO 補佐が現に属する、又は過去 2 年間に属していた事業者等

② 各工程の調達仕様書の作成に直接関与した事業者等

③ 設計・開発等の工程管理支援業者等

④ ①～③の親会社及び子会社（「財務諸表等の用語、様式及び作成方法に関する規則」（昭和 38 年大蔵省令第 59 号）第 8 条に規定する親会社及び子会社をいう。以下同じ。）

⑤ ①～③と同一の親会社を持つ事業者

⑥ ①～③から委託を請ける等緊密な利害関係を有する事業者

9 情報セキュリティ管理

（1） 情報セキュリティ対策の実施

受託者は、「別紙 13 情報セキュリティ対策の運用要件」に記載されている内容及び以下を含む情報セキュリティ対策を実施すること。また、その実施内容及び管理体制についてまとめた「情報セキュリティ管理計画書」をプロジェクト実施計画書に添付して提出すること。

① PMDA から提供する情報、もしくは本業務で知り得た情報の目的外利用を禁止すること。
② 受託者側の情報セキュリティ対策の実施内容及び管理体制が整備されていること。
③ 本業務の実施に当たり、受託者又はその従業員、本業務の役務内容の一部を再委託する先、若しくはその他の者による意図せざる変更が加えられないための管理体制が整備されていること。
④ 受託者の資本関係・役員等の情報、本業務の実施場所、本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供を行うこと。具体的な情報提供内容については PMDA と協議の上、決定するものとする。
⑤ 情報セキュリティインシデントへの対処方法（対処手順、責任分界、対処体制、対応時間、情報伝達時間・手段等）が確立されていること。
⑥ 情報セキュリティ対策その他の契約の履行状況を定期的に確認し、PMDA へ報告すること。
⑦ 情報セキュリティ対策の履行が不十分である場合、その原因について調査・排除するため、PMDA による追跡調査や立ち入り検査等について連携・協力する体制が構築できていること。また速やかに改善策を提出し、PMDA の承認を受けた上で実施すること。
⑧ 本業務に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、PMDA が必要と判断した場合は、速やかに情報セキュリティ監査を受入れること。
⑨ 本業務の役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるように上記①～⑧に関する事項を記載した情報セキュリティ管理計画書を作成し、PMDA の承認を受けること。
⑩ PMDA から要保護情報を受領する場合は、予め PMDA と合意した情報セキュリティに配慮した受領及び管理方法にて行うこと。
⑪ PMDA から受領した要保護情報が不要になった場合は、これを確実に返却、又は抹消し、書面にて報告すること。
⑫ 本業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに PMDA に報告すること。

（２） 情報セキュリティ監査の実施

① PMDA がその実施内容（監査内容、対象範囲、実施等）を定めて、情報セキュリティ監査等を行う（PMDA が選定した事業者による監査を含む。）ものとする。受託者は、あらかじめ情報セキュリティ監査等を受け入れる部門、場所、時期、条件等を「実施計画書」に付記し提示すること。
② 受託者は自ら実施した外部監査についても PMDA へ報告すること。
③ 受託者は、情報セキュリティ監査の結果、本業務における情報セキュリティ対策の履行状況について PMDA が改善を求めた場合には、PMDA と協議の上、必要な改善策

を立案して速やかに改善を実施するものとする。

④ 本業務に関する監査等が実施される場合、受託者は、技術支援及び情報提供を行うこと。

⑤ 受託者は、指摘や進捗等把握のための資料提出依頼等があった場合は、PMDA と協議の上、内容に沿って適切な対応を行うこと。

情報セキュリティ監査の実施については、本項に記載した内容を上回る措置を講ずることを妨げるものではない。

１０ 再委託に関する事項

① 受託者は、受託業務の全部又は主要部分を第三者に再委託することはできない。

② ①における「主要部分」とは、以下に掲げるものをいう。

ア 総合的企画、業務遂行管理、手法の決定及び技術的判断等。

イ SLCP-JCF2013 の 2.3 開発プロセス、及び 2.4 ソフトウェア実装プロセスで定める各プロセスで、以下に示す要件定義・基本設計工程に相当するもの。

- 2.3.1 プロセス開始の準備
- 2.3.2 システム要件定義プロセス
- 2.3.3 システム方式設計プロセス
- 2.4.2 ソフトウェア要件定義プロセス
- 2.4.3 ソフトウェア方式設計プロセス

ただし、以下の場合には再委託を可能とする。

- 補足説明資料作成支援等の補助的業務
- 機能毎の工数見積において、工数が比較的小規模であった機能に係るソフトウェア要件定義等業務

③ 受託者は、再委託する場合、事前に再委託する業務、再委託先等を PMDA に申請し、承認を受けること。申請にあたっては、「再委託に関する承認申請書」の書面を作成の上、受託者と再委託先との委託契約書の写し及び委託要領等の写しを PMDA に提出すること。受託者は、機密保持、知的財産権等に関して本仕様書が定める受託者の責務を再委託先業者も負うよう、必要な処置を実施し、PMDA に報告し、承認を受けること。なお、第三者に再委託する場合は、その最終的な責任は受託者が負うこと。

④ 受託者は、本業務の実施中に再委託先又は再委託先の要員を変更する場合は、上記項記載の要領で申請し、承認を受けること。

⑤ 再委託先が「８（２）入札制限」の要件を満たすこと。

⑥ 受託者の責任において、サプライチェーンリスクの発生を未然に防止するための体制を確立すること。

⑦ 再委託先において、本書に定める事項に関する義務違反、義務を怠った場合には、受

託者が一切の責任を負うとともに、PMDA は当該再委託先への再委託の中止を請求することができる。

⑧ 再委託における情報セキュリティ要件については以下のとおり。

- 受託者は再委託先における情報セキュリティ対策の実施内容を管理し PMDA に報告すること。
- 受託者は業務の一部を委託する場合、本業務にて扱うデータ等について、再委託先またはその従業員、若しくはその他の者により意図せざる変更が加えられないための管理体制を整備し、PMDA に報告すること。
- 受託者は再委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関して、PMDA から求めがあった場合には情報提供を行うこと。
- 受託者は再委託先にて情報セキュリティインシデントが発生した場合の再委託先における対処方法を確認し、PMDA に報告すること。
- 受託者は、再委託先における情報セキュリティ対策、及びその他の契約の履行状況の確認方法を整備し、PMDA へ報告すること。
- 受託者は再委託先における情報セキュリティ対策の履行状況を定期的に確認すること。また、情報セキュリティ対策の履行が不十分な場合の対処方法を検討し、PMDA へ報告すること。
- 受託者は、情報セキュリティ監査を実施する場合、再委託先も対象とするものとする。
- 受託者は、再委託先が自ら実施した外部監査についても PMDA へ報告すること。
- 受託者は、委託した業務の終了時に、再委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。

⑨ 上記①～⑧について、再委託先が、更に再委託を行う場合も同様とする。

１１ その他特記事項

（１） 環境への配慮

環境への負荷を低減するため、以下に準拠すること。

① 本件に係る納入成果物については、最新の「国等による環境物品等の調達の推進等に関する法律（グリーン購入法）」に基づいた製品を可能な限り導入すること。

② 導入する機器等がある場合は、性能や機能の低下を招かない範囲で、消費電力節減、発熱対策、騒音対策等の環境配慮を行うこと。

（２） その他

PMDA 全体管理組織（PMO）が担当課に対して指導、助言等を行った場合には、受託者もその方針に従うこと。

１２ 附属文書

（１） 別紙

別紙 1　審査系システムリプレイス作業スケジュール
別紙 2　審査系システムリプレイスアプリ開発要件
別紙 3　審査系システムリプレイスインフラ要件
別紙 4　審査系システムリプレイス概要図
別紙 5　審査系システムサーバー及びソフトウェア一覧
別紙 6　審査系システム構成要件
別紙 7　審査系システム移行対象資産
別紙 8　SLA（運用支援業務）
別紙 9　作業スケジュール（運用支援業務）
別紙 10　業務要件（運用支援業務）
別紙 11　その他の要件（運用支援業務）
別紙 12　システム運用管理基準
別紙 13　情報セキュリティ対策の運用要件

別紙 4、別紙 5、別紙 6、別紙 7 は本書と同時に公示される秘密保持誓約に記載及び紙面による提出を行った応札希望者に電子データで配布する。

（２） 事業者が閲覧できる資料一覧

閲覧資料 1　独立行政法人 医薬品医療機器総合機構　サイバーセキュリティポリシー
閲覧資料 2　PMDA 情報セキュリティインシデント対処手順書
閲覧資料 3　セキュリティ管理要件書(ひな型)
閲覧資料 4　医薬品医療機器申請・審査システム（Pegasus）設計資料
閲覧資料 5　申請電子データシステム（Gateway）設計資料
閲覧資料 6　eCTD v3.2.2 ビューアシステム設計資料
閲覧資料 7　eCTD v4 関連システム 設計資料
閲覧資料 8　医療機器 WEB 申請プラットフォーム（DWAP）設計資料
閲覧資料 9　治験中不具合報告管理システム 設計資料
閲覧資料 10　厚労省既承認画像検索システム 設計資料
閲覧資料 11　前回リプレイス（令和元年度）審査系システム共通基盤設計資料
閲覧資料 12　共用 LAN システム統合基盤設計資料

閲覧資料 13　統計処理業務関連資料

・統計処理業務手順書一式

・仕掛等審査費用集計業務手順書一式

・GMP 等調査実績集計業務手順書一式

閲覧資料 14　拠出金徴収管理システムにおける期末期首処理に係る資料

閲覧資料 15　オンライン専門協議用環境整備手順書

１３ 窓口連絡先

独立行政法人　医薬品医療機器総合機構　審査マネジメント部審査企画課

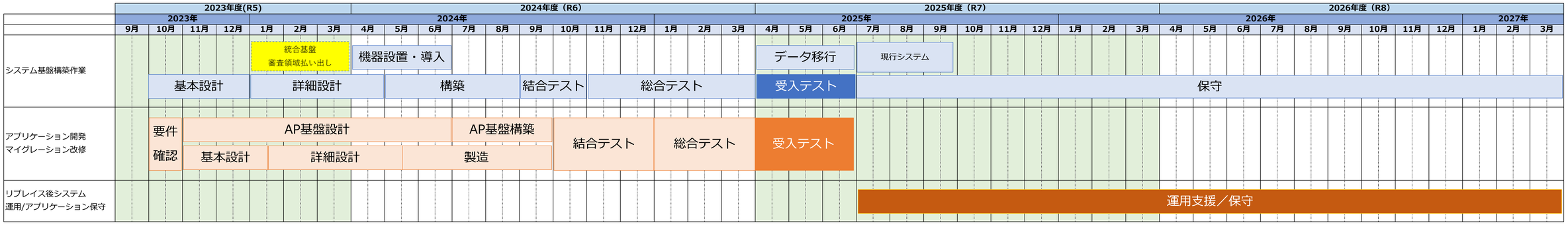
大平　泰士

電話：03 (3506) 9438

Email：ohira-yasushi●pmda.go.jp

（※迷惑メール防止対策のため●を半角のアットマークに置き換えてください。）

別紙１　審査系システムリプレイス作業スケジュール



保守契約期間はハードウェア及びソフトウェア導入日から令和12年3月31日まで

別紙２　審査系システムリプレイス　アプリケーション開発要件

1　共通

1.1　保存しているファイルの保存年限対応

Pegasus および申請電子データシステム等において、保存されているファイルについて保存年限に関する仕組みが入っていない。そのため、一定期間を過ぎたファイルについては削除領域に移すなどして一般ユーザから参照できない仕組みとし、運用支援業者やシステム管理者等の権限を保有するものが参照すると閲覧できるなどの仕組みを Pegasus の文書管理および申請電子データシステムが利用する原本区画において仕組みとして構築すること。

保存年限が過ぎたファイルを削除領域等に移動した一覧を Pegasus で閲覧可能とし、いつ、どこに保存されたファイルで、保存年限の起点日および保存年限が表示され、どのフォルダに移動されたかなどを確認できるようにすること。

なお、ファイルについては、原本区画にファイルを登録する際にファイル ID もしくはハッシュ値（SHA256 を想定）を取得し、データベースに保存するとともに、フォルダごとにマスタに設定された保存年限をデータベース上に記録することで保存年限の管理を行う。なお、通常、原本区画は読み取り専用でありファイルの移動等発生しないが、メンテナンス等で移動等行う場合は、運用手順に従ってデータベース上の情報も更新できるよう手順等整備すること。

1.2　PDF ファイルの共同編集機能

現在、申請等のオンライン化を進めている中で行政手続き上提出が必要な資料等について、今後 PDF ファイルによる提出が増えることが予想されている。提出された PDF ファイルを利用してレビューを実施するには、原本となる PDF ファイルを更新することなく、複数人が同時に資料に対するコメント等を行う必要がある。そのため、AcrobatSDK 等を用いてプラグインを作成し、ファイルを更新することなくコメント等を行えるようにすること。また、付随して対応が必要となる Pegasus の改修ついても併せて対応することになるが、具体的には以下の対応を行うこと。

1.2.1 AcrobatSDK 等用いたプラグインの開発

1.2.1.1 プラグインの開発

通常、PDF ファイルを開きコメント等を行うと PDF ファイル本体に保存されるが、AcrobatSDK にてプラグインを開発し、元ファイルに保存するのではなく Pegasus のデータベースに保存する仕組みを構築すること。なお、PDF ファイルを起動する端末から Web サーバに構

築する WebAPI をコールすることでデータのやり取りを行い、直接 PDF ファイルを起動する端末からデータベースに接続することがないようにすること。

1.2.1.2 コメントおよびハイライト、注釈機能

PDF ファイルに対するコメントやハイライト、注釈機能について、今回作成するプラグインを導入することによりファイルに直接記録するのではなく、Pegasus のデータベースに記録する仕組みとすること。なお、利用可能な注釈や編集機能を制限できるようにすること。(同時編集時に矛盾を生じやすいテキスト編集やページの挿入、削除等の禁止など。)

1.2.1.3 個人用・共有用の別機能

コメント等を登録する際に、個人用もしくは共有用として切り替えてコメント等を登録できるようにすること。この際に必要となるユーザ情報について AcrobatSDK で取得できるようにすることが望ましいが、機能上の制限などによりユーザ情報を取得できない場合は、ユーザ情報を取得するための代替手段を検討し PMDA に説明した上で、PMDA と協議の上対応すること。なお、代替手段においてはユーザ側が自身のユーザ情報を書き込むなど、コメント等を登録時にユーザ側に負荷がかからないような仕組みとすること。

1.2.1.4 プロパティ情報追加機能

開いた文書に対してプロパティ情報を登録できるようにすること。この際に、プロパティの項目名と値を登録できるようにするが、最大 10 個登録可能とすること。項目名については汎用マスタ管理機能 (発行・失効管理が可能な汎用マスタ) にて追加や削除を行えるようにし、ファイルを開いたときに汎用マスタ管理機能から項目を呼び出し設定できるようにすること。プロパティ情報は、個人用と共有用で区別できる仕組みとすること。

1.2.1.5 WebAPI をコールする際の認証および認可機能

認証とは AcrobatSDK から WebAPI にコールする際に本人確認を行う仕組みとし、PDF ファイルを起動した端末にログインしている共用 LAN 端末の ID を WebAPI のパラメータに含めることで、Pegasus 利用ユーザであることを判別できるようにすること。

また、認可とは当該ユーザが Pegasus で管理しているグループ機能で許可されているグループに所属していることを管理できるようにすること。

1.2.1.6 同時編集機能

当該機能を用いてコメント等を行う際に、複数ユーザが同時に同じPDF ファイルを編集できるようにすること。なお、別ユーザが同一個所にコメントやハイライトを行っている個所に対してコメント等を付して保存しようとした場合は、メッセージウィンドウを表示し保存できないようにすること。この際に、複数コメント等を行っているものの、他ユーザが編集していない箇所については保存を完了させるようにし、重なって保存しようとしている個所のみ保存できないようにすること。

1.2.1.7 再表示機能

AcrobatSDK で開発するプラグインとして、再表示機能を設けること。これにより、再度データベースから他ユーザがコメント等をした内容を読み込みし表示できるようにすること。この際に、自身が編集中のコメント等は削除せず残したままとするが、読み込むことで同一個所を他ユーザが編集しているものがある場合は、メッセージウィンドウを表示するなどして、編集が重なっていることをユーザに知らせ、許可した場合に再表示するような機能とすること。

1.2.1.8 プラグインの展開について

PMDA 役職員へのプログラムの展開は共用 LAN で提供しているWindows の「ソフトウェアセンター」を用いて展開することを想定しており、展開するためのインストーラの作成なども本業務に含まれるが、展開方法等含め詳細については担当者と調整の上対応すること。

1.2.1.9 コメント付きファイルの保存

付与された個人用または共有用コメントを表示した状態の PDF ファイルを出力（別名で保存）できること。出力したコメント付き PDF ファイルは、開発するプラグインなしの Acrobat Reader で閲覧可能とすること。

1.2.2 Pegasus 機能改修

1.2.2.1 登録されたコメント等の検索機能

AcrobatSDK を通して登録されたコメントやハイライト箇所などについてはデータベースに保管されることになるが、それらについて個人用・共有用の別やファイル名、コメントの文言、プロパティ項目とその値などの検索条件を指定し検索可能とすること。また、検索した結果の一覧から検索した文書にリンク等で直接開けるようにすること。その際に、既存の文書検索機能が存在するため統合した形で実現すること。なお、技術的に統合することが難しい場合は、PMDA に説明の上、別途機能を構築すること。

1.3　リスク評価、監査対応

リスク評価および監査における指摘事項等についてシステム側で対応すべき以下の事項について対応すること。

1.3.1 大量データ取得時の際にアラート出力する機能を追加すること。対象は以下の機能とする。

(1)　Pegasus

アラート出力する機能は、「素データ出力」、2022 年度　拠出金システムの審査系システムへの移行及びオンライン申告対応改修業務で開発している「汎用検索機能」、1000 件越えを許容している検索機能（例えば、審査品目検索や承認等品目台帳検索機能など)。

(2)　申請データシステム

ゲートウェイ提出画面、送信テスト画面、ファイル送信画面(FD 申請・届出等)、ファイル送信画面(FD 申請様式外提出）試験データ提出、試験データ提出(改訂)の各画面

1.3.2 アプリケーションやジョブプログラムで NAS 等の機器の特権アカウントを使用する場合は機器標準のアカウントではなく、専用のアカウントを別途作成すること。

1.3.3 特権 ID とパスワードについて管理簿を作成する際はすべての ID/パスワードを一つのファイルに載せるのではなく、業務システムや機器の種類（サーバ、ネットワーク機器等）の区分ごとに分割し、それぞれ限定された者のみが開くことができるようにすること。また、機器類やサーバ、ミドルウェア等に対する権限付与、はく奪等のスクリプトを自動で生成できるようにし、また、自動で生成できるようにした機器類等から自動で情報を取得できるようにする機能を作成すること。自動化にあたっては、コマンドラインで対応できる範囲について実施すること。

1.3.4 バックアップデータを使用した復元訓練（※）を実施できるよう運用手順を定め、検証環境にてその手順に従って問題なく訓練が行えるようにすること。
※仮想サーバやデータベース、物理サーバ、ファイルなどについてすべてダメになったことを想定し、すべてバックアップからレストアできるようにするための手順を定め訓練可能とする。

1.3.5 Pegasus 等が使用するデータベース（SQL Server）について、アプリケーションアカウント・バッチアカウントを除くアカウントでデータベースへの接続をリスト化し、日時の確認と接続用途のヒアリングを接続者に行うなど、データベースへの不正な操作を発見する仕組み（データベースサーバの監査証跡機能等）を構築すること。

1.4　最新の OS、ミドルウェア、ソフトウェア対応

各システムにて使用している OS やミドルウェア、ソフトウェアについては、現行使用している製品のバージョンアップ版、もしくは後継製品を使用することになるが、本契約で購入した製品について、別紙１　審査系システムリプレイス作業スケジュールに示すリプレイス後システム運用/アプリケーション保守期間中に発生するサポート期間終了に伴うバージョンアップを行い、現在利用している機能が問題なく稼働するよう対応すること。その際に、以下の点についても漏れなく対応すること。

1.4.1 保守契約期間内に販売終了することが判明している製品については後継製品もしくは代替製品を適用し連接するシステムについてもプログラム改修や設定変更等行い現行満たしている機能を実現すること。なお、後継製品や代替製品の制約により満たせない機能がある場合は、PMDA に相談の上、PMDA の指示に従うこと。

1.4.2 導入した製品が保守契約期間内にサポートが終了するが、その後バージョンアップする場合においては、バージョンアップ版もしくは後継製品を無償で提供すること。なお、バージョンアップした製品の適用作業については本業務の範囲外とするが、適用するための手順書の提供や手順通りにならなかった場合の対応などの情報提供は本業務の範囲内とする。

1.4.3 各種 OS やミドルウェア、ソフトウェアのバージョンアップに伴い発生する各システムのプログラム修正については、現在利用している機能が問題なく稼動するように対応すること。本対応は、別紙１　審査系システムリプレイス作業スケジュールに示すアプリケーション開発及びマイグレーション改修期間に発生する作業が対象であり、リプレイス後システム運用/アプリケーション保守期間中に発生する作業については、アプリケーション保守の工数を使用して対応すること。

1.5　資産管理ソフトの変更対応

現在、Subversion を使用して設計書やプログラム資産を管理しているが、分散開発をしやすくするため、Git に変更し今後の管理を行えるよう、導入および手順等を整備すること。

1.6　各アプリケーションなどで使用しているアカウントの整理

今回のリプレイスに伴い不要なアカウントは削除し、利用するアカウントのみとするよう対応すること。併せて利用するアカウントのクレデンシャル情報をシステム内に保存する場合は暗号化するよう対応すること。なお、技術的な問題などで暗号化が難しい場合については PMDA に説明の上、PMDA の許可を得るこ

と。

1.7　令和５年度～令和６年度で実施する予定の改修内容について、令和５～６年度に実施する下記案件において実施された改修内容について当該リプレイス案件においてマージを行い当該案件としてリリースすること。なお、下記以外にも緊急の案件などで改修が発生する可能性がある。それら案件における改修内容を５０人月の範囲でマージを行いリリースすること。

1.7.1 令和５，６年度審査系統合運用保守業務

1.7.2 令和５年度 Pegasus 改修業務（緊急承認制度対応、都道府県における参照権限拡大、業許可システム台帳表示仕様変更）

1.7.3 令和５年度拠出金オンライン化対応

1.7.4 令和 5, 6 年度審査系システム汎用化等機能追加開発業務

2　Pegasus

2.1　オンライン文書レビューの部署別データベース管理廃止対応

現在のオンライン文書レビューは、部署ごとにデータベースがわかれており、それぞれ容量が定まっている状況である。しかしながら、部署が追加されるなどした場合、追加しづらい状況にあるため、１つのデータベースとして、その中に各部のフォルダを作成する方式に変更する。なお、各部に設定している自動削除期限などは保持したままとし移行すること。

3　申請電子データシステム

3.1　全体試験・品目横断 DB の刷新

全体試験・品目横断 DB について臨床試験の実データを取り込むのではなく、以下のような臨床試験のメタデータのみを取り込み、申請名や試験名を検索するシステムに作り替える。

・申請情報から取得する情報（分野、販売名、効能・効果、投与経路、申請者名、提出日、申請日、承認日、申請区分、等）

・CDISC 規格の臨床試験データから取得する情報（試験名、相、DM ドメインの情報（被験者数、対象年齢、等）、TS ドメインの情報（Endpoint、主要評価項目、ランダム化、盲検化、トライアルデザイン情報、等）、define.xml の情報（規格及び辞書のバージョン、等）、等

3.2　現在、ログイン時に電子証明書による本人認証を行い、さらにファイル送信時にも同電子証明書を付している状態であるが、ファイル送信時の電子証明書選択を

取りやめ、すべて SkeedWebGo による送信となるように対応すること。そのため、現在 SkeedWebGo において電子証明書選択をしないような改修を行い、かつ、現在.Net アプリを使用して送信している機能も WEB 画面から直接アップロードできる仕組みに改修し、SkeedWebGo による送信が可能となるよう改修すること。また、その時にファイルが送信されたものであることを証するため、セッション ID 等を同時にファイル送信し、バッチ処理する際にレコードに別途保存しているセッション ID と突合させ、その時に送信したファイルであることの確認を行うよう改修すること。

なお、SkeedWebGo にはファイル送信中における「改ざん検知機能」が備わっているため、SkeedWebGo の当該機能を ON とするための対応も行うこと。

4　eCTDv3.2.2

個別要件はないため、「共通」項に記載している 1.3（ただし 1.3.1 を除く）から 1.7 の内容のみ対応すること

5　eCTDv4

5.1　ビルド環境の統合

現在、Pegasus や eCTDv3.2.2 とのバージョンの違いによりビルド環境を統一できていなかったが、今回のバージョンアップに伴い、Pegasus や eCTDv3.2.2 と IDE やビルド環境を統一すること。

6　DWAP

個別要件はないため、「共通」項に記載している 1.3（ただし 1.3.1 を除く）から 1.7 の内容のみ対応すること

7　拠出金管理システム

個別要件はないため、「共通」項に記載している 1.3（ただし 1.3.1 を除く）から 1.7 の内容のみ対応すること

8　既承認画像検索システム

個別要件はないため、「共通」項に記載している 1.3（ただし 1.3.1 を除く）から 1.7 の内容のみ対応すること

9　上記要件を満たすためにシステムの整合性の観点から必要となる既存機能の改修において適宜改修内容含め PMDA に説明の上、PMDA と調整すること。

別紙３　審査系システムリプレイスインフラ要件

1.　ハードウェア及びソフトウェア要件

統合基盤外で使用するハードウェアと、統合基盤及び調達するハードウェア上で使用するソフトウェアを調達する。導入を想定するハードウェア及びソフトウェアの詳細は「別紙6　審査系システム構成要件」及び「別紙５ 審査系システムサーバー及びソフトウェア一覧」を参照のこと。なお、提案する構成に応じて機器やライセンスの追加等が必要な場合は、導入ハードウェア及びソフトウェアに含めること。

1.1.　共通事項

製品サポートの観点で、本業務に関わるシステムのライフサイクル（システム利用期間の終了又は本契約期間の終了迄）におけるサポート（交換部品、セキュリティパッチの提供等）を継続し受けられる製品を選定すること。サポートライフサイクルポリシーが事前に公表されていない製品を納入する場合は、サポートが継続して行われるように後継製品への更新計画を提出すること。後継製品に更新する場合の製品購入費用及び更新作業費用（アプリケーション改修は除く）は本業務に含むものとする。なお、提案する各ソフトウェア製品等について、現時点で製造元がライフサイクルを公表していない、または、本業務の契約満了までの保守費用の確定ができない等の事由がある場合において、後継製品に更新する際の費用が現行製品と比べて大きく増減する場合や、後継製品が販売されない等のやむを得ない理由で更新できない場合には、ライフサイクルが公表された時点で、変更管理により要件（ソフトウェアのライセンス数、保守の有無、等）の変更等の対応について別途協議を行うものとする。

また、「14.保守要件」、「17.信頼性要件」、等の要件を考慮して製品を選定すること。

納品対象には、製品に付属する取扱説明書、並びにシステム環境の構築及び運用・保守作業に利用する製品仕様や操作手順等に係る日本語で書かれたドキュメント類を含むものとすること。その他ドキュメント類に関しても、納品に際してはその内容（使用言語等）を説明の上、PMDA の承認を得ること。

1.2.　ハードウェア

オープンなシステム環境の整備を可能とするため、選定する製品は以下に示す規定等に準拠していること。また、これらに準拠した製品に対する必要十分なインターフェースを有すること。

・ITU-T（国際電気通信連合）あるいは ISO（国際標準化機構）等が規定又は推奨する各種国際標準に準拠していること。

・装置の製造・データ処理に関しては、IEEE（米国電気電子技術者協会）等が規定又は推

奨する各種デファクトスタンダードに準拠していること。
・全て未使用品を納入すること。また同一要件の物品においては全数を同一機種にて納入すること。

1.3. ソフトウェア

・ボリュームライセンス、ガバメントライセンスの適用を考慮すること。
・ソフトウェアパッケージ間の連携を考慮した上で、動作保証できるソフトウェアパッケージの組み合わせとすること。
・検収後に、製品の使用についてライセンス規約に適合しないことが認められた場合は、受注者の責任において、その権利の使用に必要な費用の負担及び使用許諾契約にかかる一切の手続きを行うこと。ただし納品後にソフトウェア販売元によりライセンス規約が変更された場合はこの限りではない。

2. 環境の要件

本業務で導入する環境は、大きく以下の 2 種類とする。

2.1. 本番環境

本番サービスが稼働する環境として利用する。

2.2. 検証環境

テスト等を実施する環境として利用する。

2.2.1. 用途

・アプリケーションソフトウェアの結合テスト、総合テスト、受入テストを実施する。
・障害発生時における再現テスト、障害調査・分析、プログラム等の改修・検証、外部システム又は PMDA 内の他システムとの連携検証等を実施する。
・セキュリティパッチ適用、ソフトウェアバージョンアップによる変更の影響調査を行う。
・本番環境へのリリースに際して、事前検証を行う。

2.2.2. 構成

・プログラム及びソフトウェアパッケージは、本番環境と同等の製品及びバージョンとすること。
・システムリソースについては、本番環境と同規模である必要はないが、論理的に三面の並行環境状態に耐えうる規模とすること。
・冗長化については、本番環境の構成を踏襲することが望ましい。
・テスト及び保守作業等を並行して実施できるように、Pegasus、申請電子データシステム、eCTD v3.2.2 ビューア、eCTD v4 関連システムについては、論理的に 3 つの面に分割すること。

3. 機器設置及び設備要件

導入するハードウェアは、PMDA が指定する日本国内のデータセンター及び新霞が関ビル内に設置すること。設置に関し、要求する事項を以下に示す。

3.1. データセンター

・統合基盤が提供する EIA 規格の 19 インチラックに、ラックマウントキットを用意して機器を設置すること。
・統合基盤が提供するネットワークスイッチ及びネットワークケーブルに、10GBASE-SR に対応したネットワークアダプター及びトランシーバを用意して機器を接続すること。
・200V 電源に対応した冗長電源装置及び電源ケーブルを用意して機器を接続すること。

3.2. 新霞が関ビル

・EIA 規格の 19 インチラック及びラックマウントキットを用意して機器を設置すること。
・統合基盤が提供するネットワークスイッチ及びネットワークケーブルに、10GBASE-SR に対応したネットワークスイッチ、ネットワークアダプター及びトランシーバを用意して機器を接続すること。
・100V 電源に対応した UPS 装置をラック内に設置し、冗長電源装置及び電源ケーブルを用意して機器を接続すること。

4. ネットワーク環境要件

4.1. 基本事項

本業務で構築するシステムは、統合基盤が提供する PMDA 内のネットワーク上に配置すること。また、本番環境と検証環境のネットワークは論理的に分離すること。厚生労働省、地方厚生局、各都道府県との接続には医薬品等専用ネットワークを利用すること。

実装については、統合基盤が提供する FW、IPS、スイッチ等のネットワーク機器について、設計・構築・テストを実施すること。

5. 監視要件

障害の早期検知及び対応の早期化を実現するために、統合基盤が提供する監視サーバー（Zabbix）を利用すると共に、Logstorage が稼働するログ管理サーバーを導入し、機器及びソフトウェアの異常を検知できるようにすること。なお、構築中における総合テスト以降（運用支援期間含む）において、ログ等で異常とするものであっても、システム上影響のない異常が含まれることがある。そのようなものについては異常検知対象外とし、対象外一覧

として整理すること。監視項目は以下とする。

・ICMP 死活監視
・リソース監視(CPU/Memory/Storage/traffic)
・SNMP trap
・syslog、イベントログ監視
・ELC/SBT
・アプリケーションログ
・特定フォルダのファイル操作

6. セキュリティ要件

6.1. 基本事項

「医薬品医療機器総合機構情報サイバーセキュリティポリシー」に準拠した情報セキュリティ対策を講じること。また、本受託者は、最新の「政府機関のサイバーセキュリティ対策のための統一基準」、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」及び「「高度標的型攻撃」対策に向けたシステム設計ガイド」、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」を参照の上、必要に応じてその内容を取り込むこと。このほか、審査系システムに係る情報セキュリティ要件は、「閲覧資料 1 医薬品医療機器申請・審査システム(Pegasus)設計資料」及び「閲覧資料 2 申請電子データシステム(Gateway)設計資料」に示す。

6.2. 情報セキュリティ対策

「別紙 13　情報セキュリティ対策の運用要件」を実現する機能を実装すると共に、以下について対応すること。

6.2.1. 情報セキュリティ機能の実装

・業務上必要なアクセスに限定すると共になりすましを防止するための利用者認証機能及び、当該機能を検証するために使用する令和 9 年 3 月末迄有効なクライアント証明書
・伝送データを暗号化する機能及び、暗号化用に組み込む契約期間内に有効なサーバー証明書
・テープバックアップデータを暗号化する機能
・権限を持つ PMDA 職員が、利用者の画面操作に関するログを参照又は分析するための不正追跡機能
・権限を持つ PMDA 職員が、特権 ID を利用したすべての保守及び運用に関する作業証跡を参照又は分析できる、特権 ID 不正追跡機能
・サーバー、ストレージ等に対する不正アクセス等の監視を行うための不正監視機能
・ブラウザ経由にて想定される Web アプリケーションに対する不正アクセス（クロスサ

イトスクリプティング、SQL インジェクション等）対策機能
・あらかじめ検知対象に定義されたフォルダ配下の不正な変更を検知する、改ざん検知機能
・ウイルス、スパイウェア等の不正プログラムを検知し、駆除又は隔離を行うとともに、定義ファイルの自動配布・適用を行う不正プログラム対策機能
・セキュリティレベルの異なるネットワーク境界上にて、ネットワーク間で行われる通信の通過制御を行うファイアウォール機能
・ネットワーク、サーバー等に対する不正アクセスを検知、遮断し、警告を通知する不正侵入防御機能
・ネットワーク、サーバー等に対するサービス不能化の攻撃を検知、遮断し、警告を通知する不正アクセス対策機能
・導入するサーバー類に対してソフトウェアをインストールされた際に自動で検知し、システム管理者にメール等で通知すると共に、定期的にインストールされたソフトウェアの増減を管理できる機能

6.2.2. 脆弱性対策の実施

・原則として、導入するハードウェア及びソフトウェア、統合基盤から提供され本業務で設計及び構築する全ての構成要素に対し、脆弱性対策を実施すること。
・原則として、導入するハードウェア及びソフトウェア、統合基盤から提供され本業務で設計及び構築する全ての構成要素に対し、公表されている脆弱性情報及び業務期間中に公表される脆弱性情報を収集する手順を整備すること。
・本業務に基づくシステム構築が影響する範囲について、第三者による脆弱性検査を実施し、その結果を PMDA に書面にて報告すること。脆弱性検査は PMDA 内経由とインターネット経由の両面から実施すること。なお、インターフェースシステム等、他機関より提供され改修することなく実装するソフトウェアや、統合基盤においてテスト不可となる機器等については、脆弱性検査の対象外とする。
・脆弱性検査の結果、明らかになった不具合等は、速やかに修正を行うこと。なお、不具合によりスケジュールに大きな影響がある場合や、設計書等に不具合が発見された場合は速やかに PMDA に報告し、適宜調整の上対応方針を検討すること。

6.2.3. 情報セキュリティ対策の履行状況の報告

本業務の遂行におけるセキュリティ対策の履行状況について、PMDA から報告を求めた場合には速やかに提出すること。

6.2.4. 情報セキュリティ監査への対応

・PMDA が第三者機関等による情報セキュリティ監査を受ける場合には、PMDA を支援すること。情報セキュリティ監査の結果、対策が必要な場合は、PMDA と協議を行い、合意した対策を実施すること。

・本業務の遂行において、本受託者における情報セキュリティ対策の履行が不十分であると認められる場合には、本受託者は、PMDA の求めに応じ、PMDA と協議を行い、合意した対応を実施すること。

6.2.5. IT セキュリティ評価及び認証制度に基づく認証取得製品の採用

ハードウェア、ソフトウェアパッケージ等のすべての構成要素については、「IT セキュリティ評価及び認証制度」に基づく認証を取得している製品を積極的に採用すること。

6.2.6. サプライチェーン・リスクへの対応

IT 調達に係る申合せ（「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」）に留意し、採用予定の製品については、予め PMDA にリストを提出し、PMDA がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、PMDA と迅速かつ密接に連携し提案の見直しを図ること。

6.2.7. 管理体制の整備

納入する基盤製品について、不正が見つかったときに、追跡調査や立入検査等により原因を調査・排除できる体制を整備していること。

7. 構成管理要件

・SKYSEA Client View の資産管理機能を用い、機器の構成情報を管理する機能を実装すること。
・情報資産台帳は PMDA が指定するフォーマットを使用し、ソフトウェア一覧、ハードウェア一覧、ライセンス一覧などの必要な情報を記載すること。
・検証環境内の SVN 又は Git を用い、各種ドキュメント(設計書等)やソースコードのバージョンを管理する機能を実装すること。

8. バックアップ要件

バックアップは、障害発生等に伴い失われるデータの回復、ユーザーエラーからの回復を目的として行うものとする。統合基盤が提供するバックアップ機能及び本業務で構築する新霞が関ビル内のバックアップ機能（バックアップサーバー、テープ装置、Arcserve）を用いて、以下要件を実装すること。

・バックアップ取得時間

業務データ（アクセスログを含む。）のバックアップは、原則として運用時間終了後の夜間帯に行うものとする。データベースのバックアップは 30 分ごとにトランザクションログのバックアップを行い、障害から 30 分前以内の状態にリストア可能とすること。

・システム設定変更時のバックアップ

システムバックアップの取得は、ハードウェア構成の変更、ソフトウェアパッケージに対するパッチの適用等のシステム変更時において、原則、審査系ヘルプデスクが手動で行うものとする。

・バックアップ方式

バックアップは、原則としてオンライン方式で取得するものとする。

・バックアップ保存期間

バックアップデータは、2 世代以上保持することを基本とし、データの種類及び特性に合わせてバックアップ保存期間を規定すること。テープメディアへの長期保存を目的としたバックアップデータの保存期間は永年とする。

・遠隔地保管

災害等に備え、バックアップを遠隔地の保管場所へ定期的に輸送するので、その輸送を可能とするよう、テープメディアに業務データやシステムバックアップ等を出力する。

9. 業務アプリケーションのマイグレーション対応

サーバーOS、データベースソフト、システムで使用するその他ソフトウェア等について、サポート期限終了等に伴いバージョンアップを行う。ただし旧法システム内の仮想サーバーについては、現行のソフトウェアバージョンを継続使用する。導入を想定するソフトウェアの詳細は「別紙 5 審査系システムサーバー及びソフトウェア一覧」を参照のこと。バージョンアップ後に現行と同様の機能が維持できるよう、各アプリケーションのマイグレーション対応を実施すること。

また、本システムと接続する調達範囲外システムとの接続およびテスト等を実施するため、必要な設定変更およびテスト支援を行うこと。

10. 設計要件

10.1. 基本事項

本インフラ要件全般についての設計を行うこと。現行システム基盤の構成をもとに統合基盤に移行し、また本紙及び「別紙 6 審査系システム構成要件」の要件に沿って現行システムを一部変更するために必要な設計を行うこと。各設計については、PMDA の承認を得た上で基本設計から詳細設計等以降の作業に進むこと。設計作業に際して PMDA の保有する設計資料等の資産が必要な場合は、PMDA に提示を要求すること。PMDA は開示可否を検討した上で、開示可能と判断したものについては本受託者に公開するので、それを基に設計作業を行い作業の効率化を図ること。

基本設計の主な項目を以下に記す。

システム構成

- ├物理構成
- ├論理構成
- ├ソフトウェア構成
- ├回線一覧
- ├外部接続システム

システム基盤方式設計

- ├命名規則
- ├セキュリティ
- ├可用性
- ├拡張性
- ├サーバー
- ├ネットワーク
- ├ストレージ
- ├バックアップ・リストア
- ├監視
- ├ジョブ
- ├ウイルスチェック
- ├アカウント管理

ネットワーク設計

- ├セグメント
- ├IP アドレス
- ├ルーティング
- ├ファイアウォール
- ├負荷分散
- ├冗長性
- ├通信経路
- ├セキュリティ

IPS 設計

WAF 設計

サーバー設計

- ├サーバー一覧、機能一覧
- ├ハードウェア一覧
- ├可用性、冗長化方式
- ├ユーザーアカウント
- ├OS
- ├ソフトウェア

仮想基盤設計
ストレージ設計
　├論理構成
　├ゾーニングとアクセス方式
　├可用性
　├冗長化方式
バックアップ・リストア設計
監視設計
ログ管理設計
ジョブ管理設計
構成管理設計
本番環境／検証環境間のデータ受け渡し設計

10.2. 統合基盤との役割分担

統合基盤が提供する機能については「別紙 6 審査系システム構成要件」を参照のこと。

11. 構築要件

11.1. 基本事項

本システムで必要となる各種環境について、設計書に基づいて構築作業を行う。構築作業の際には、必要となる情報を整理した上で、導入手順書を作成すること。

11.2. 統合基盤との役割分担

統合基盤が提供する機能については「別紙 6 審査系システム構成要件」を参照のこと。統合基盤が提供する機能について、製品導入作業は統合基盤側が実施し、導入後の設定作業を本受託者が実施する。なお、一部統合基盤が選定する機器等において直接設定作業を実施できない場合が生じる可能性がある。その場合は統合基盤担当者と調整し、設計や設定値等の共有、統合基盤担当者が設定した後のテスト等を実施すること。

12. テスト要件

12.1. 基本事項

実施する単体テスト、結合テスト、総合テスト、受入テストについて、共通となる要件は以下のとおり。

・審査系システムの正常稼働を保証するためのテストとして、単体テスト、結合テスト及び総合テストを実施すること。また、PMDA が行う受入（運用）テストの支援を行うこと。

・各テストを行うため一連のテストケース（入力、出力、及びテスト合否基準)、テストデータ、及びテスト手順を整理し、テスト計画書として作成し、PMDA と協議の上、承認を得ること。
・各テスト終了時に、実施内容、品質評価結果、及び次工程への申し送り事項等について、テスト結果報告書を作成し、PMDA と協議の上、承認を得ること。
・テストに使用するテストツール等については、PMDA と協議の上、使用すること。

12.2. テスト計画

実施する単体テスト、結合テスト、総合テストについて、設計し、テスト方針、実施内容、及び実施理由を記述し、テスト計画書として提示し、テスト開始 1 ヶ月前までに PMDA と協議の上、承認を得ること。

承認されたテスト計画書に基づき、進捗管理を確実に実施すると共に、進捗状況の報告を定期的かつ PMDA の求めに応じて行うこと。

以下に、テスト計画書で必要と考える事項を示す。

テスト概要
　├テスト範囲（各テスト工程におけるテストの概要を含む）
　├テスト品質目標（テスト項目数、不具合検出数）
テストに関する実施作業及びスケジュール
テスト環境（テストに使用した回線及び機器構成、その他ツール、場所等）
テスト体制（テスト実施者、テスト結果確認者（評価者））
使用及び提出するドキュメントとその定義
　├テスト項目一覧
　├テスト仕様書
　├懸案事項一覧
　├テスト結果報告書

12.3. 単体テスト

プログラム及びモジュールが個別単体において例外処理含め正しく機能することを確認する。パッケージ化されたプログラム及びモジュールについてもテスト範囲とする。パッケージ化されている範囲について単体テストを実施しない場合には、実施しなくても該当機能が正しく機能することを別の手段で証明し、PMDA と協議の上、承認を得ること。

12.4. 結合テスト

プログラム及びモジュールが、審査系システムの各システムの単位でそれぞれ正しく機能することを確認するため、段階的に結合した状態でテストを行い、ソフトウェアの結合が完全であることを確認する。

12.5. 総合テスト

審査系システム全体として要件どおりにシステムが構築されていることを確認するためにテストを行い、システムが納品可能な状態であることを確認する。確認に当たっては、ソフトウェア製品が仕様に適合し、かつ実稼働環境で利用可能であることを確認できる評価指標及び合格条件を設定した上で、テストを実施する。脆弱性診断テストについても、ここで行う。

特に、総合テストにおける性能及び負荷のテストにおいては、想定する最大人数が同時に利用開始した場合であっても問題が生じないことを確認する。

12.6. 受入テストの支援

PMDA が実施する受入テストにおいて、本受託者は、テスト計画の策定、準備、テストの実施、成果物の作成、テスト実施結果の報告等に関して、基盤製品に関する設定変更、情報提供等の必要な支援を行うこと。

12.7. テストデータ及びその取扱い

本受託者が主体的に実施するテスト（以下、テスト工程）においては、本受託者が準備したテスト用データを使用すること。PMDA のデータ（以下、本番データ）を元にテストデータを作成する場合は、マスキング等の加工を施すこと。本番データをマスキング等の加工をせずテストに使用する場合は、必要性等を PMDA に説明し、PMDA の承諾を得て使用すること。なお、テスト工程における本番データの管理責任は本受託者が負うこと。

特に、外部接続を行うテストにおいて本番データを使用する場合は、外部にデータが漏洩しないことが前提となる。そのため、外部接続を行うテストにおいては、アプリケーションおよび機器等の設定を確認し、さらに、スタブモジュール等を作成するなど、本番データにアクセスできないような施策を講じること。なお、外部接続を行うテストにおけるテスト方針およびデータの取り扱い等については、テスト計画時に PMDA と協議の上取り決めを行うこと。

PMDA が主体的に実施するテスト（以下、受入テスト）においては、本番データを使用することになり、その管理責任は PMDA が負うことになる。ただし、受入テストにおける操作ではなく、本受託者の操作等により漏洩等のインシデントが発生した場合はその限りではない。

12.8. 不具合の修正

テストの結果、明らかになった不具合等は、速やかに修正を行うこと。なお、不具合によりスケジュールに大きな影響がある場合や、設計書等に不具合が発見された場合は速やかに PMDA に報告し、適宜調整の上対応方針を検討すること。

テストで検出した不具合に関しては、原因究明と分析・対策・水平展開を実施し、その結果を報告書として提出すること。

設計・構築時に定めた設定パラメータについて、PMDA が実施するテスト段階において

不具合が発生し、要件を満たさない場合は、見直しを行うことがある。その場合、本受託者は見直しの支援と設定変更作業を行うこと。

13. 移行要件

13.1. 基本事項

現行システムから更改後のシステムへの移行に当たっては、機器の安定稼働及び業務の継続に影響を与えることなく、速やかに実施する必要がある。以下の基本事項に基づき、移行計画・作業を行うこと。

・審査系システムの安定した稼働及び業務の継続に影響を与えることがないよう、安全で確実な作業を優先すること。

・PMDA が承認した日時を除き、現在稼働中のシステムのサービスを停止することなく、移行作業を行うこと。

・システムの停止を伴う作業が避けられない場合には、システム利用者への影響を最小限に抑えるため、平日においては、勤務時間外、その他土日及び休日を作業実施日の基本として検討し、停止予定日より、原則 1 ヶ月前に停止日時及び停止による影響（停止するサービスの範囲）について、PMDA の承認を書面にて得ること。

・移行作業中に障害が発生した場合には、速やかに原因究明にあたるとともに、移行実施計画書、システム切替手順書に従い、切り戻し作業を行い、PMDA の承認を得て、必要な障害対処作業を本受託者の責任と負担により実施すること。

・移行の実施前に、現行機器のデータについて、バックアップを取得すること。

・本業務での対応に伴い、厚生労働省、地方厚生局、各都道府県が審査系システムとの接続に使用している医薬品等専用ネットワーク利用者側に設定変更が必要となる。設定変更作業は厚生労働省、地方厚生局、各都道府県で実施するため、設定に必要な情報の提供を行うこと。

13.2. 移行手順

移行において想定する作業は以下のとおり。

① 移行計画書の策定
② 移行設計
③ 移行手順の作成・検証
④ 移行プログラムの作成・検証
⑤ リスクの洗い出し・コンティンジェンシープランの作成
⑥ 移行リハーサルの実施
⑦ 移行判定
⑧ 移行作業の実施

13.3. 移行対象データ

審査系システムで管理しているファイルやデータベース、設定などを含む情報全てを移行対象データとする。ただし PMDA が移行不要と判断したデータについては除外する。移行対象データの規模は、「別紙 7 審査系システム移行対象資産」を参考とすることができるが、当該規模は令和 4 年 9 月時点のものであるため、業務開始時に改めて移行対象データ規模を確認すること。

14. 保守要件

14.1. 共通事項

・調達する全てのハードウェア及びソフトウェアを保守の対象とする。

・ハードウェアに組み込まれたファームウェア及びハードウェアに付随するソフトウェアも全て保守の対象であり、切分けを含む故障対応、問い合わせ対応及びライセンス更新等を実施すること。

・必要に応じて統合基盤が導入したハードウェア又はソフトウェアとの切分けを実施すること。

・調達するハードウェア又はソフトウェアに起因することが明らかな障害が発生した場合を除き、PMDA と共同で障害の切分けを実施すること。

・セキュリティホール等の情報及び対策のためのパッチやアップデートファイル等を入手可能であること。また、パッチ等の適用について技術的な情報を提供すること。

・PMDA からの問い合わせに対して、技術支援を行うこと。

・マニュアル上に記載されていない等の理由により、運用管理事業者が対応出来ない事項に対する回答を行うこと。

・保守期間

令和 12 年 3 月 31 日まで

・保守時間

平日（土曜日、日曜日、「国民の祝日に関する法律」で定められた休日及び 12 月 29 日から 1 月 3 日までを除く）9 時～17 時とする。（該当する保守メニューが存在しない場合を除く）

14.2. ハードウェア

・障害発生時及び PMDA からの問合せ時に迅速な対応が出来る体制を取り、障害の連絡から 4 時間以内に保守要員を派遣すること。ただしシステムの冗長化が図られ、継続運用が可能な場合は、PMDA と協議し、対応を決めることが出来ることとする。

・保守サービスの内容により予兆検知が可能な場合は、障害の予兆を発見した時点で保守対応を開始すること。

・PMDA 職員の指示のもと、機器の障害の復旧作業を行うこと。
・機器の修理、故障部品の交換が必要な場合は、機器の設置場所で行うこと。
・情報漏出を防止するため、記憶装置の障害発生等で部品交換が必要になった場合、故障したハードディスク等の記憶媒体は回収せず、PMDA の指示に従うこと。
・機器のファームウェアの更新に係る情報を入手し、提供すること。また、ファームウェアの適用について技術的な情報を提供すること。
・ハードウェアに関する仕様等の基本情報、及びその他製品に関する技術情報を提供すること。
・機器を安定稼働するために予防保全として、定期点検を年 1 回程度行うこと。

14.3. ソフトウェア

・障害発生時及び PMDA からの問合せ時に迅速な対応が出来る体制を取り、連絡に対して速やかに回答を行うこと。
・アップデートプログラムに係る情報を入手し、提供すること。また、アップデート作業について技術的な情報を提供すること。
・OS、ミドルウェア等のソフトウェアについて障害が発生した場合は、原因解析を行うこと。ソフトウェアの不具合であった場合には、ソフトウェアメーカーと保守契約を結ぶことで提供される保守の範囲でパッチやソフトウェアのアップデート、設定変更等により復旧すること。パッチやソフトウェアのアップデート、設定変更等によりアプリケーションの機能に影響を及ぼす場合には、PMDA 職員と対応について協議すること。

15. 性能要件

現行仕様及び関連資料を確認し、現行から著しく劣ることがないようにすること。本システムの性能に関する要件は、以下に示すとおりである。

15.1. オンライン処理応答時間

以下にレスポンスタイム及びターンアラウンドタイムの要件について示す。遵守率は 90%以上とする。
・審査系システムのレスポンスタイムは、全て 1 秒以内とすること
・画面遷移を伴うターンアラウンドタイムは、全て 5 秒以内とすること
・文書ファイルの表示、検索等に関わるターンアラウンドタイムは、全て 5 秒以内とすること
・外部から申請電子データを受信し、ウイルスチェック後の Ack を送信したタイミングから、データストレージ機能にて臨床試験データ原本ファイルの複製が完了するまでの処理時間が 2 時間以内であること
・上記に関わらず、ファイルやデータのサイズに依存する処理、高負荷となる処理及び処

理件数の変動幅が大きな処理等、応答時間の要件を満たすことが困難なケースについては、PMDA と協議の上、個別に定めるものとする。

本業務において求めるレスポンスタイム及び、ターンアラウンドタイムに係る考え方を「図 4-1」に示す。ここで、レスポンスタイムとは、ノードごとのサーバー内部処理時間とし、ターンアラウンドタイムとは、利用者が端末を利用して処理要求を送ってから、すべての結果が出力されるまでの時間とする。

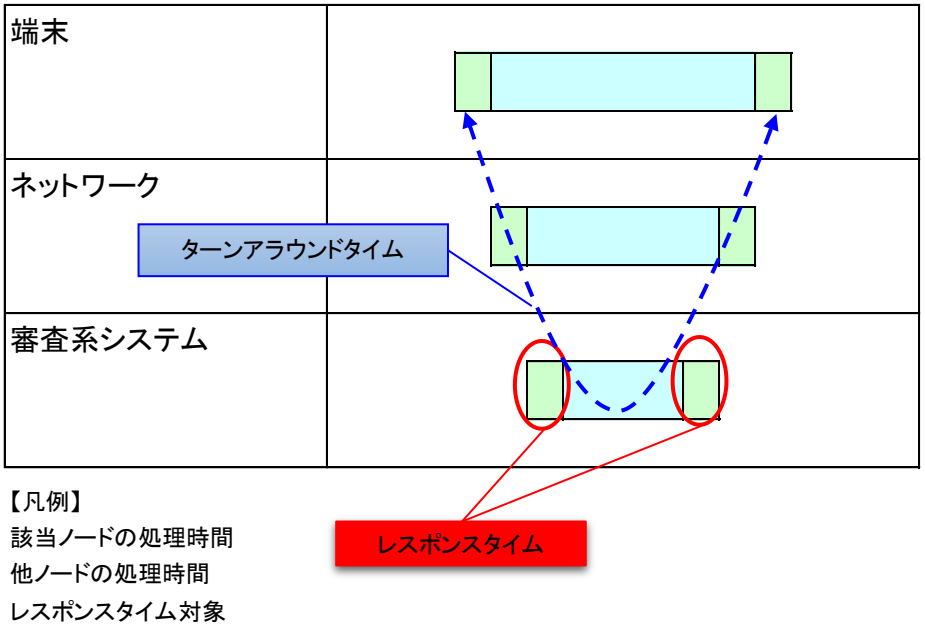


図 3-1　レスポンスとターンアラウンドタイムのイメージ

15.2. バッチ処理

オンラインの稼働時間中に実施するバッチ処理については、オンライン／ディレイドオンライン業務サービスとの同時処理を可能とし、かつオンライン処理のレスポンスタイムに影響を与えないようにすること。

16. 信頼性要件

16.1. 基本要件

・計画停止時間及びメンテナンス時間を除いて、24 時間 365 日稼動が可能であること。
・ハードウェア及びソフトウェアは、法人向けに販売されている実績のある製品を選定すること。
・機器等に採用するパーツ類については、メーカー保証品とすること。
・本業務で構築するシステムと同等の規模（トランザクション量とデータ量）での使用実

績があること。なお、業務量に依存しない製品については対象外とする。
・障害が発生した場合、復旧時に障害発生の直近にバックアップされたデータ及び設定を回復できること。
・業務終了後の運用支援等を本受託者によらず、これを行うことが可能となるようドキュメント類の整備を行うこと。
・オープンソースソフトウェアの製品やツールについては、当該製品の保守や技術サポートを調達することが困難である場合は、採用しないこと。なお、当該製品を組み込むために、審査系システムのすべて又は一部のソースコードを開示する必要が生じる場合は、事前に PMDA と協議すること。

16.2. 可用性

16.2.1. ハードウェアの構成可用性に係る目標値

可用性に係る目標値を「表 3-1」に示す。

表 3-1　審査系システムの SLA

No.	SLA 項目	説明	設定値
1	サービス稼働時間	・審査系システムのサービスが提供される時間帯 ・定期保守、法定停電等による停止時間を除く	24 時間 365 日
2	運用・保守サービス時間	・運用・保守サービスのうち、監視業務、障害対応業務が提供される時間帯	平日：9:00～17:00 土日祝日：対応しない
3	稼働率（正常稼働時）	・No.1 に示すサービス稼働時間における稼働予定時間に対して実際に稼働した時間（稼働時間）の割合であり、以下の式により計算する ＜稼働率（%）＝（1－1 ヶ月の停止時間÷1 ヶ月の稼動予定時間）×100＞ ・ 稼動予定時間とは、定期保守、法定停電等による計画した停止時間を除く、1 ヶ月に稼動すべき時間である ・ 停止時間とは、サービスが停止していると確認された時刻（本業務で導入する監視機能で障害を検知した時刻、または、利用者が連絡した時刻のいずれか早い方）から利用可能とされた時刻までの経過時間を指す ・ 停止時間には、待機系システム等への切換えのために発生した停止時間、障害からの本各復旧のために必要になった停止時間、人為的なミスにより発生した停止時間等を含む ・ 冗長化構成されている部分のうち、一部分が停止した場合でも、冗長化によりサービスの提供に支障を来たさなかった場合には、停止時間として取り扱わ	99.5%以上

		ない ・ PMDA 側に責任があることが確認できた場合には、停止時間として取り扱わない ・障害検知時刻が審査系ヘルプデスク提供時間外の場合、経過時間は翌営業日のヘルプデスク提供時間開始後から起算する	
4	稼働率（縮退稼働時）	・ 冗長化構成がされている部分のうち一部分が停止した場合で、レスポンスタイムの低下等が生じている時間（縮退稼動時間）を停止時間として取り扱う ・ 縮退稼動時間とは、縮退稼動の開始から正常稼動に復旧するまでの時間とするが、PMDA の都合により正常稼動への復旧作業を延期する場合等は、復旧のための準備がすべて整い、PMDA の承認を得るまでの時間を縮退稼動時間とする ・ 上記以外は正常稼働時と同様	96.0%以上
5	レスポンスタイム(正常稼働時)	・ すべての個別サービスが稼動しており、対象となる利用者がログインしている状態で、対象となる個別サービスすべてにおいて（外部インターネット接続を除く）、利用者が何らかの処理を行った後、システムが処理を行い、再度、利用者に操作が委ねられるまでの時間 ・ 本条件を満たすことができない処理がある場合には、構築期間において、本受託者がその根拠・考え方（各システムの標準的な動作環境、前提等）を提示し、PMDA の承認を得ること ・ クライアント PC 内での処理時間がアプリケーションのレスポンスに影響を与える場合は、クライアント PC 内での処理時間を排除した実績を計上することも可とする	5 秒以内
6	レスポンスタイム(縮退稼働時)	・ 冗長化されている部分のうち、一部分が停止した場合に許容するレスポンスタイム ・ 上記以外は、正常稼働時と同様	7 秒以内
7	平均故障間隔（MTBF：Mean Time Between Failure）	・ システムに故障が発生してから、次に故障が発生するまでの平均時間で、以下の式により計算する ＜平均故障間隔＝総稼動時間÷総故障件数＞ ・ 個別サービスの稼動状態（停止、縮退稼動、及び通常稼動等）に関らず、特別な対応が 必要になるすべての故障・不具合を故障件数として取り扱うこと ・ PMDA 側に責任があることが確認できた場合には、故障件数として取り扱わない	2920 時間（4 ヶ月）以上
8	平均復旧時間	・ 平均復旧時間とは、ヘルプデスク稼	6 時間以内

	（MTTR：Mean Time To Repair）	動時間中において、機器に故障が発生した時刻から故障が復旧した時刻までに要した時間の 1 ヶ月間における平均値である ・ 平均復旧時間は、以下の式により計算する ＜平均復旧時間＝1 ヶ月の総復旧時間÷1 ヶ月間の総件数＞ ただし、平均復旧時間の計算には、ヘルプデスク稼動時間外を含まないものとする ・故障が発生した時刻とは、本業務で導入する監視機能で障害を検知した時刻、または、利用者が連絡した時刻のいずれか早い方とする ・復旧とは、障害原因を排除し、正常に稼働することを確認し、利用者が使用可能な状態にあることとする（縮退運転等の暫定復旧も復旧とみなす） ・ PMDA 側に責任があることが確認できた場合には、復旧時間計算の対象から除外する	
9	RPO（目標復旧時点）	・データの損失は許容できないため、データの再送や再処理を含め、障害発生時までの復旧を基本とする（大規模災害時を除く）	データの障害： 障害発生時 機器等の障害： 直近のバックアップ時点 大規模災害時： 1 ヶ月以内
10	RTO（目標復旧時間）	・業務停止時間を極力少なくするため、6 時間以内の復旧を目標とする（大規模災害時を除く）	データの障害： 6 時間以内 機器等の障害： 10 時間以内 大規模災害時： 数ヶ月以内

16.2.2. 可用性に係る対策

・本業務で導入する機器等は、性能劣化や停止により業務処理が影響を受けることのないよう、冗長化を行うこと。なお、サーバーの冗長化に当たっては、可能な限り Active-Active 構成とし、サーバー間の負荷がなるべく均等になるように処理を分散して割り当てるとともに、機器資源の有効活用を図ること。

・Active-Active 構成で冗長化したサーバーは縮退運転を可能とし、その場合のレスポンス順守率は 60%とすること。

・ストレージは、ハードディスク等故障時のデータ消失対策として、ホットスワップ可能な RAID 構成とすること。またホットスペア用ディスクを搭載すること。

16.3. 拡張性

導入するハードウェアの構成要素(メモリ、ハードディスク等)及びソフトウェアのライセ

ンス数について、拡張が可能であること。ハードウェア構成要素の拡張性については、初期導入時の 1.5 倍以下を目安とする。

16.4. 上位互換性

本業務の範囲内のハードウェア、OS、ソフトウェア、ミドルウェア、その他パッケージソフトウェア、ネットワーク関係機器等は、運用期間を通じて継続的にサポート（部品交換、バグフィックス、セキュリティパッチのリリース等）が保証される製品を選定すること。また、メーカーから情報や資材の提供を受け、バグフィックス、セキュリティパッチの適用等、必要となる措置を行うこと。

16.5. システム中立性

・採用する技術や製品については、原則、将来にわたり市場等で代替技術・技術者等を容易に調達できるよう配慮すること。
・競争原理によって、適正な価格で調達することが可能な製品であること。
・他の業者においても、市場で調達可能な製品であり、本受託者が独占的に供給する製品ではないこと。
・特定の技術及び製品に依存せず、高品質・高信頼と経済性を兼ね備え、継続的に提供される技術を適用可能なハードウェア及びソフトウェアとすること。
・本システムの次期更改時の移行作業において、特定の業者、製品に依存することなく円滑に移行実施可能なシステム構成であること。
・審査系システムのための独自仕様でないこと。

16.6. 事業継続性

16.6.1. 目標値

大規模災害（地震、火災及び風水害等又は第三者による情報システムへの攻撃等による直接的な設備及び情報システムの損壊、あるいは、ライフライン（電力、通信及び交通等）の機能不全による情報システムの長時間停止）が発生した場合を除いて、審査系システムを用いた業務処理が維持できること。

16.6.2. 対策

大規模災害が発生した場合に対しては、早急にその状態を把握し、リスクの拡大を防止し、速やかに回復させるための処置を講じることとして、その対策を運用計画書及び保守計画書に取りまとめること。

16.7. データの保守

審査系システムが管理する業務データについては、原則永年保存とする。出力されたログについてはログ管理ソフトウェアが収集する。容量及び運用面で効率的にログを保管するために、保存期間は 1 年とする。

17. 現行システム機器撤去および返却、廃棄の要件

17.1. データ消去

機器の再利用が可能な方法（データの上書き等）で現行機器のデータ消去を実施すること。また、作業完了後にデータ消去作業完了報告書 兼 データ消去証明書を提出すること。

17.2. リース返却に伴う搬出

データ消去作業済の機器をラックから取り外し、同一拠点内の PMDA が指定する一時保管場所にケーブル含め移設すること。その後、現行の機器提供業者と運搬方法および運搬場所等について調整の上日本国内の指定する場所に運搬すること。なお、既設ストレージ内の一部ディスクはリース返却および廃棄の対象外であるため、PMDA が指定するディスクを除いた上で搬出を行うこと。PMDA が指定するディスクは東京都内の PMDA が指定する場所に運搬すること。

17.3. データセンターの原状復帰

ラックから機器を取り外した後、受託者の負担においてデータセンターの原状復帰を実施すること。

17.4. 廃棄

現行機器が設置されている場所にあるリース返却対象外の機器及びケーブル類（サーバ部品等含む）は、「独立行政法人　医薬品医療機器総合機構サイバーセキュリティポリシー」に基づき、電磁的記録の抹消・破壊等の適切な措置を講じた上で廃棄し、廃棄証明書を発行すること。

18. 運用に関する事項

本業務で構築する全てのハードウェア、ソフトウェア及びネットワークを対象に運用業務を行うための運用設計を行うこと。また、現システム構成で作成されている運用計画書、運用手順書、操作手順書、保守計画書、保守手順書等のドキュメント類を本業務で構築した基盤や構成に合わせて整備すること。

なお、現システム構成において一部サーバー等においてパッチ適用をオンラインで適用できるよう手順を整備しているところであるが、すべて手動で整理している状況であり自動化ができていない。そのため、本業務内において以下の観点で自動化の可否について検討し、PMDA と協議した上で可能な限り自動化を行うこと。

・ロードバランサー配下の仮想サーバーに対してパッチ適用をする場合、仮想サーバーに対してセッションを確立しないようにし、セッションがなくなった段階でロードバランサ

ーから切り離した後パッチ適用を行い、再びロードバランサーの対象とすること

・WSFC などのクラスタ構成を取っているサーバー群に対してパッチ適用をする場合、パッチ適用する対象のサーバーへの接続をさせず、セッションがなくなり次第切り離しを行ってからパッチ適用をし、パッチ適用後クラスタ構成に戻すこと

・シングルポイントのサーバーに対してパッチ適用をする場合、任意のタイミングもしくは特定のタイミングにおいて自動でパッチ適用を行うこと

19. 教育に関する事項

ソフトウェアのバージョンアップによる変更に起因して、大幅な運用変更は発生しない想定である。しかしながら、「別紙 2 審査系システムリプレイスアプリ開発要件」で改修する内容においては少なからず業務影響が発生するため、「別紙 2 審査系システムリプレイスアプリ開発要件」で改修する内容含め、PMDA 内の利用者と申請者側の利用者に対し、各 1 回程度変更点を抜粋した説明用資料を作成すること。

なお、運用期間中に発生する保守工数における改修において、説明会の実施は求めないが、利用者向けの説明資料作成の依頼があった場合は、説明用資料を作成すること。

20. 引継ぎに関する事項

以下の事項に留意して、運用・保守業者等に引継ぎを実施すること。なお、引継ぎ先、引継ぎ内容及び手順等の概要を、「表 4-2 引継ぎ内容、手順」に示す。

・運用・保守業務の円滑な実施に役立つよう、必要な各種情報及び資料の提供を行うこと。

・引継ぎの内容は、事前に PMDA に示し承認を得ること。

・PMDA 及び引継ぎ先と日程を調整した上で実施すること。

・引継ぎに必要な資料等は、本受託者において用意すること。

・必要に応じて、実機での操作説明等を行うこと。

表 3-2　引継ぎ内容、手順

No.	引継ぎ発生時（予定）	引継ぎ元	引継ぎ先	引継ぎ内容	引継ぎ手順
1	令和 9 年 3 月	本受託者	審査系システム運用業者	本仕様書のインフラに係る運用手順等について、本受託者及び PMDA が必要と判断した引継ぎを行うこと。	・引継計画書を策定すること。 ・引継計画書に基づき、引継ぎを実施し、引継ぎ実施後、引継ぎ完了報告書を作成すること。

別紙8 「SLA(Service Level Agreement)項目」

No	指標の種類	指標名	目標値	計算式・計測方法・評価基準	計測周期
1	システム運用	サーバおよび機器可用性	冗長化されているノード: 月間 99.9% 冗長化されていないノード: 月間 99%	・ (各監視対象ノードが稼働している時間の延べ時間)÷(各監視対象ノードが稼働すべき時間の延べ時間) ・ ハードウェアおよびミドルウェアが正常稼働している場合、稼働している時間とみなす。 ・ 評価対象ノードは物理サーバ、仮想サーバ、ネットワーク機器、ストレージ装置とする。 ・ 評価対象時間は、平日 9:30～18:00 の時間帯とするが、参考情報として平日 9:30～18:00 以外の時間帯も計測する。 ・ システムの提供時間は、原則 24 時間 365 日とする。 ・ 予め計画されたサービス停止、コールドスタンバイのように予め想定されるノードダウンは除き、稼働すべき時間とする。 申請電子データシステムにて業務利用されているサーバ等のメンテナンスを実施する場合は、原則として利用停止の 5 週間前までに外部ユーザに連絡可能な日で PMDA 職員と調整する。 ・ 申請電子データシステムにて業務利用されているサーバ等以外のメンテナンスを実施する場合については、緊急の場合を除き、作業を実施する 5 営業日前までに PMDA と調整する。 ・ ネットワーク障害に起因し、ノード監視が出来ない場合もサーバダウンとみなす。	毎月
2	システム運用	レスポンス	遵守	・ 以下の応答速度を達成する。 画面応答(参照系)3 秒 画面応答(更新系)3 秒 ※1 DB 検索結果表示 3 秒 ※1 DB 更新処理 3 秒 ※1 文書ファイル表示 5 秒 ※1 文章ファイル検索結果表示 3 秒 ※1 文章ファイル全文検索結果表示 3 秒 ※2 ファイル更新(アップロード、ダウンロード)10 秒以内 ※3 なお、VPN 経由のアクセス、100 件以上のダウンロード、1MB 以上のファイル送受信、複雑な組合せでの検索などについては、以下の条件とする。 ※1:10 秒 ※2:30 秒 ※3:60 秒 ・ 遵守状況の報告のみ。定量的報告は不要。	毎月

No	指標の種類	指標名	目標値	計算式・計測方法・評価基準	計測周期
3	システム運用	データ保全性	遵守	・ バックアップについては、下記を要件とする。なお、下記が満たせない場合は都度状況を報告し、PMDA 担当者の指示に従い、対応をすること。 仮想サーバ:メンテナンスの都度1世代取得(手動) 物理サーバ:メンテナンスの都度1世代取得(手動) NAS ファイル:1回/1日(自動) 遠隔地保管(仮想サーバ):1回/1日(自動) 申請審査 DB トランザクションログ:1回/30 分(自動) 各種アプリ、機器等のログ:常時、1 年保存(自動) ・ データのリカバリについては、下記を要件とする。 ◇データ障害 RPO(目標復旧時点):障害発生時(最大 30 分前) RTO(目標復旧時間):6 時間以内 ◇サーバ障害 RPO(目標復旧時点):前回取得バックアップ時点 RTO(目標復旧時間):10 時間以内 ◇災害 RPO(目標復旧時点):前回取得バックアップ時点 RTO(目標復旧時間):機器、データ等必要部材が揃った状態から1か月以内。 ・ 遵守状況の報告のみ。定量的報告は不要。	毎月
4	システム運用	障害通知	遵守	・ 障害発生時刻から 30 分以内に確実に PMDA 職員に連絡をとり応答を得る。 ・ データセンタに設置されたハードウェア及びソフトウェアにて発生した障害については、障害検知後の一次切分けにてデータセンタでの作業が必要と判断した後、180 分以内にデータセンタへ入館し、一次切分け作業を開始出来ること。 ・ 障害発生時刻がヘルプデスク提供時間内の場合に限るが、提供時間外だった場合は、翌営業日のヘルプデスク提供時間開始後 30 分以内に初動開始とする。 ・ 遵守状況の報告のみ。定量的報告は不要。 ・ 一次切分け作業の結果、及び状況については、原因の特定有無にかかわらず 1 時間以内に行うこと。	毎月

No	指標の種類	指標名	目標値	計算式・計測方法・評価基準	計測周期
5	システム運用	障害復旧遵守率 （4.5 時間以内）	95%	・ （障害発生時刻から、障害復旧までの経過時間が 4.5 時間以内の件数） ÷（発生障害件数） ・ 対象は影響レベル 3 以上のインシデントとする。 ・ データパッチ、代替手段の提供、縮退運転などの暫定対応も障害復旧とみなす。 ・ 障害発生時刻がヘルプデスク提供時間外の場合、経過時間はヘルプデスク提供時間開始後から起算する。	年間
6	システム運用	障害原因切分け遵守率 （翌営業日以内）	80%	・ （障害発生の当日又は翌営業日に障害原因切分けが完了した件数） ÷（発生障害件数） ・ ハードウェア障害、ミドルウェア障害の場合はベンダ問合せを行うこと、アプリケーション障害の場合は、対応方針を決定しシステム管理者へ報告することを以って障害原因切分け完了とみなす。	毎月
7	ヘルプデスク	問合せ回答率 （翌営業日以内）	80%	・ （問合せ受付の当日又は翌営業日に、回答が完了した件数）÷（問合せ受付件数） ・ 問題解決につながる回答を行った時点で回答完了とする。 ・ 作業依頼の連絡については除外する。	毎月
8	ヘルプデスク	ヘルプデスク提供時間	遵守	・ 平日 9:30-18:00 まで。ヘルプデスク業務に支障をきたさないように調整した上で、1時間の休憩時間をとる。 ・ 行政機関の休日（「行政機関の休日に関する法律」（昭和 63 年法律第 91 号）第 1 条第 1 項に掲げる日をいう。）を除く日とする。 ・ 要員別作業項目別に月間の作業時間を集計し、月次にて報告すること。	毎月
9	セキュリティ	重大障害の件数	0 回／年	・ 下記に例示するような重大なセキュリティインシデントを発生させない。 サーバ上で不正プログラムが実行される等の方法による、データの破壊や改ざん。 FAX やメール等の機構外への誤送信。 機密情報（申請情報など）の第三者への漏洩。 書類、PC、IC カードなどの紛失。 ・ システムで利用する製品等について、セキュリティ情報の公開から、5 営業日以内にセキュリティパッチ適用等の検討を完了する。 セキュリティ情報は以下のサイト等から取得し、検討対象となったセキュリティインシデントおよび情報取得元、 検討内容および対応方針等を取りまとめ、PMDA に報告し、対応内容については PMDA の指示を仰ぐこと。 ・ https://jvn.jp/ ・ https://www.jpcert.or.jp/ ・ https://www.meti.go.jp/policy/netsecurity/index.html	毎月

別紙9　作業スケジュール（運用支援業務）

■システム改修業務を除く運用・保守支援業務のスケジュール(案)

No	項目	実施区分	令和7(2025)年									令和8(2026)年													令和9(2027)年			実施内容
			4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	
マイルストン																											
1-1	キックオフ	実施 ◎				▲																					実施計画書に基づくキックオフを実施する。
1-2	前業者からの引継ぎ	実施 ◎	実施																								契約後2週間以内に運用準備作業に関する実施計画書（運用準備作業）を作成し、PMDAの承認を受けた後、前事業者からの引継ぎを行う。
1-3	月次定例	実施 ◎				▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	
1-4	次年度(新業者)への引継ぎ	実施 ◎																								実施	
1-5	成果物納品	実施 ◎																								▲	
運用																											
2-1	インシデント一覧報告 （ｼｽﾃﾑ障害、情報ｾｷｭﾘﾃｨｲﾝｼﾃﾞﾝﾄを含む）	報告 ○				▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	「システム運用標準」 ⇒インシデント管理：インシデント一覧による月次報告
2-2	システム変更作業報告 （パッチ適用状況報告を含む）	報告 ○				▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	「システム運用標準」 ⇒変更管理：変更作業一覧による月次報告
2-3	特権ID使用状況報告 （台帳を含む）	報告 ○				▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	「システム運用標準」 ⇒特権ID管理台帳・特権ID使用管理簿による月次報告
2-4	データ保全（バックアップ）状況の点検	報告 ○				▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	「システム運用標準」 ⇒バックアアプと回復：遵守状況の月次報告、机上訓練（任意）
2-5	情報セキュリティ：遵守状況の報告	報告 ○				▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	「システム運用標準」 ⇒情報セキュリティ：遵守状況の報告
2-6	脆弱性対策の実施状況の点検	報告 ○				▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	⇒情報セキュリティ管理：セキュリティパッチ適用状況の報告 脆弱性に関し関する新着情報、影響度・適用要否、適用予定と実績
2-7	統計処理業務	実施 ◎				▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	年集計	▲ 月集計	▲ 月集計	前年度集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	年集計	▲ 月集計	▲ 月集計	
2-8	仕掛審査等費用集計業務	実施 ◎				▲ 月集計	▲ 月集計	▲ 月集計	今年度半期集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	前年度集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	今年度半期集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	▲ 月集計	
2-9	GMP等調査実績集計業務	実施 ◎								今年度半期集計					前年度集計								今年度半期集計				
2-10	医療機器承認品目一覧作成業務	実施 ◎						実施			実施			実施			実施				実施			実施			実施	
2-11	拠出金徴収管理システム期末期首処理支援	実施 ◎													実施	実施	実施										業許可情報や承認品目の取得、取込み等を実施する。
システム保守業務																											
3-1	アプリケーション保守	実施 ◎				実施																					審査系システムアプリケーションの保守改修。あらかじめ定めた保守工数の範囲内で、案件ごとに都度期間を定めて実施する。
3-2	アップデート作業	実施 ◎				実施																					ハードウェア・OS・ミドルウェア等のセキュリティパッチ、アップデートプログラムの適用。適用タイミングは適宜調整。
3-3	試験データバリデーションルールの変更に伴うシステム変更	実施 ◎				実施																					必要に応じて随時
その他業務																											
4-1	審査知識データベース維持・管理業務	実施 ◎				実施																					(1)PMDAが作成した審査報告書等の審査知識をデータベース化する業務 (2)将来的な審査系システムへの統合を視野に入れた、当該データベースを作成・活用するためのデータベース管理ツール（プログラム）の作成・維持・管理（改修等を含む）
権限管理																											
5-1	各業務データアクセス権限再検証	支援 △						準備	実施			▲ 報告									準備	実施			▲ 報告			不要なアクセス権限の洗い出しと削除を行う。
5-2	ユーザーID棚卸し	実施 ◎						準備	実施			▲ 報告									準備	実施			▲ 報告			不要IDの洗い出しと削除・無効化。不要なID、権限があれば削除する。
5-3	特権ID検証(棚卸し)	実施 ◎				準備		実施	▲ 報告									準備			実施	▲ 報告						【システム運用標準】"システム運用管理(要件書)"に基づく運用 ⇒台帳と使用管理簿の相関チェック、使用管理簿とログの相関チェック

No	項目	実施区分	令和7(2025)年 4月	5月	6月	7月	8月	9月	10月	11月	12月	令和8(2026)年 1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	令和9(2027)年 1月	2月	3月	実施内容
点検																											
6-1	情報資産棚卸し・リスク評価	支援 △				準備	実施			▲ 報告							準備		実施			▲ 報告					⇒　厚労省のガイドラインに従って実施：「情報資産台帳」「情報資産ライフサイクル確認様式」「リスク評価チェックシート様式」の作成・更新を行う。
6-2	システム台帳の最新化	支援 △						準備	実施			▲ 報告															⇒資産台帳・管理簿(システム台帳)を更新する。 ⇒ネットワーク機器ソフトウェア資産台帳を更新する。
6-3	ログ取得状況の点検	支援 △						準備	実施	▲ 報告										準備	実施	▲ 報告					⇒情報資産の重要度に応じて、監視対象となるイベントを絞り込み、ファイル抽出した上で、セキュリティ違反を示す証跡がないかを定期的に確認する。
6-4	セキュリティヘルスチェック（不正プログラム及び不正な設定変更の有無確認）	支援 △				準備	実施	▲ 報告										準備	実施	▲ 報告							
6-5	情報セキュリティ：遵守状況の自己点検	実施 ◎														準備	実施	▲ 報告									「システム運用標準」 ⇒情報セキュリティ：遵守状況の報告
6-6	情報システム開発・運用資料確認	実施 ◎										準備	実施	▲ 報告										準備	実施	▲報告	情報システムの開発・運用・保守に必要な各種ドキュメント（各種設計書、手順書等）と実装（システムの構成・設定、プログラム等）が一致していることを確認する。
教育・訓練																											
7-1	システム運用担当者向けセキュリティ研修	受講 △										受講												受講			開催時期および開催方式は未定。
監査																											
8-1	委託先における情報セキュリティ対策の履行状況の確認	受査 ◎						準備		受査											準備	受査					PMDAが検査を実施する（開催時期は未定）。
PMDA監査受査への支援																											
9-1	厚労省・情報セキュリティ監査	支援 △						監査支援													監査支援						開催時期は未定。
9-2	調達による第3者情報セキュリティ監査	支援 △							監査支援													監査支援					開催時期は未定。
9-3	監査指摘対応フォロー	支援 △					運用フォロー					▲ 報告	運用フォロー					▲ 報告	運用フォロー					▲ 報告	運用フォロー		「過去（平成27･28･29年度）の監査対応状況について」に基づく進捗管理、半期毎に報告する。

別紙 10　業務要件（運用支援業務）

業務の時期・時間の定義

	実施時期・期間	実施・提供時間	補足
通年	令和７年７月１日～令和９年３月３１日 ※支援業務を行う日は、本書で別途定められている業務の他は、行政機関の休日（「行政機関の休日に関する法律」（昭和 63 年法律第 91 号）第 1 条第 1 項に掲げる日をいう。）を除く日とする。	9:30～18:00 ※12:00～13:00 は休憩時間とする。ただし、問い合わせや障害の発生状況、緊急メンテナンスなどの状況に応じて、交代で休憩の時間帯を適宜変更することは問題ない。	ただし、本書で別途定めるものの他、緊急作業及び本業務を実施するために必要な作業がある場合は、この限りではない。

運用業務の範囲定義

No.	名称	役割・概要
1-1	① サービスレベル管理	「別紙８　SLA」に基づき、サービスレベル管理を実施すること。サービスレベルの達成状況についてサービスレベル報告書としてとりまとめ、定例の報告会を通じて報告すること。サービスレベルが遵守できなかった場合、その改善策（手続きや体制の見直し、新たなツールや仕組みの検証・導入等）の検討・実施を必須とする。ただし、設計内容や製品仕様、開発事業者や保守事業者など、運用管理事業者自身以外に起因しサービスレベルを遵守できない場合はその旨を報告する。また、改善策の実施状況や改善の状況について、定例会を通じて報告すること。
1-2	② 稼働統計確認集計	月次にて、稼働統計情報を収集し報告と評価を行うことで、リソース（CPU、メモリ、ディスクなど）拡充が必要となる時期を予め察知できるようにする。稼働統計情報としては、OS リソース、ストレージリソース、DB リソース、ネットワークリソースなどの情報を取得する。
1-3	③ 計画停止	システム運用にあたり、メンテナンスや新霞が関ビルの計画停電の対応のために、計画停止が必要なケースがあり、この時に業務推進に与える影響を最小限とするために、作業計画の策定およびシステム停止のアナウンスを行う。例えば、Pegasus を停止することとなった場合は、申請電子データシステムや DWAP に影響が及ぶことになるため、各システムに与える影響と利用者に与える影響等勘案し、審査全体としてもっとも影響の少ない横断的なメンテナンス計画を立てる必要がある。 なお、セキュリティパッチ対応については、冗長化を行っていないサーバ以外はシステムを無停止で適用等行うこと。（冗長化を行っていないサーバであっても、リアルタイムに利用されておらず、ジョブ等を止めることでシステム停止を回避できる場合は、その限りではない。）また、データベース更新を伴わないプログラムリリースについては、原則としてシステムを無停止でリリースすること。
1-4	④ バックアップ／リストア	インシデント発生の際などに備えデータのバックアップが行われる。バッチ処理により定期的に自動取得する場合と、手順により不定期に手動取得する場合がある。総合職員が必要と判断した際は、ヘルプデスクは手動でのバックアップ取得およびリストアを実施する。

No.	名称	役割・概要
		新霞が関ビル内のバックアップ用テープドライブがあるが、その LTO 交換を週次で行い、外部倉庫ワンビシへ運搬し保管する。 また、半年に 1 回程度、各種サーバのシステム領域およびネットワーク機器の構成情報等、PMDA が指定する対象のバックアップを手動で取得すること。 なお、テープにラベルを貼りつけ、テープ内のデータ概要（受付番号など、ファイルが紐づく属性およびデータの種類）や保管場所などを管理すること。
1-5	⑤ セキュリティ対策	ア　監査対応 監査室からの内部監査および監査法人からの外部監査が実施される。その際、監査者の求めに応じて、監査証跡、各種ログ、ユーザ一覧などを取得または整理し提示する。また、必要に応じて事前打ち合わせへの出席、監査者からのヒヤリングに適宜出席すること。監査者からの質問に対し、システム的な背景、業務的な背景を踏まえた適切な回答を行う必要があるため、高いレベルでのシステム知識、業務知識が求められる。 イ　セキュリティ対策の対応状況棚卸し NISC（内閣官房情報セキュリティセンター）の公表する基準（「政府機関等のサイバーセキュリティ対策のための統一基準群」等）を遵守して運用されることが求められる。基準の改訂があった際に新しい基準に対する対応状況の棚卸しを行う。 ウ　情報収集 不正プログラムや暗号化アルゴリズムの危殆化情報について、最新の情報を取得するように努め、月次にて報告を行う。ただし、NISC などから緊急の注意喚起があった場合は即時報告し、対応する。
1-6	⑥ 運用監視	以下の４つの方法で障害検知を行う。 ｌ 各システムの運用監視ツールおよびシステム機器上で入手可能なログ ｌ データセンタ事業者からの障害連絡 ｌ HW/SW ベンダからの障害連絡 ｌ 平日業務開始時に行うヘルプデスクの日次確認作業 障害検知した際は、事前に取り決めたプロセスに従い対応を行う。 基本的には Logstorage からのエラー検知により対応を行うが、無視してもよい検知内容である場合、同様のエラー等については今後アラートが上がらないよう対応を行うこと。
1-7	⑦ 障害対応／セキュリティインシデント対応（障害原因調査を含む）	事前に取り決めたプロセスに従い、検知した障害に対し、平日日中であればヘルプデスクが主体となり対応を行い、休日や夜間帯であれば PMDA 職員が主体となって対応する。緊急性が低いと判断された障害については翌営業日にヘルプデスクが対応する。なお、障害がアプリケーション障害の場合においても、受託者のシステム知識・業務知識により障害の解析を行い、業務に支障をきたさないよう、データ修正等の暫定対応を行うこと。 障害／セキュリティインシデントを検知した場合、又は PMDA より障害／セキュリティインシデントの連絡を受けた場合には、発生箇所の一次切分けを行い PMDA と協議の上、障害発生箇所のサポート契約先に連絡し、必要に応じて各作業者の立会い及び支援作業（ログ収集、起動・停止，バックアップデータの提供、軽微な設定変更作業等）を行うこと。データセンタに設置されたハードウェア及びソフトウェアにて発生した障害については、障害検知後の一次切分けにてデータセンタでの作業が必要と判断した後、180 分以内にデータセンタへ入館し、更なる切分け作業を開始出来ること。サポート契約のない箇所の障害と判明した場合は、PMDA と協議の上、障害復旧作業の支援を行うこと。ハードウェア保守業者による機器交換

No.	名称	役割・概要
		等の作業が発生した場合は、データセンタでの作業の場合はリモートによる支援とし、新霞が関ビルでの作業の場合は作業に立ち会うこと。なお、一次切り分け作業の結果報告、及び状況報告については、原因の特定有無にかかわらず、1 時間以内に行うこと。障害発生箇所の一次切り分け以降の対応は、下記「保守業務の範囲定義」に基づく。なお、障害対応が完了されるまで管理・報告等を行うこと。 また、本業務として行ったすべての障害検知及び障害対応について、その要旨（障害日時、対象システム、障害分類、障害内容等）の記録を作成すること。 セキュリティインシデントが発生した際は、迅速なエスカレーションが求められ、関係者へのアナウンスを行う。 なお、対応を行うにあたり、申請電子データシステムの操作に必要となる個人電子証明書は、ヘルプデスク業務体制に応じて必要量購入すること。なお、購入した電子証明書の納品は不要とする。
1-8	⑧ 作業依頼対応	ユーザや管理者からの作業依頼として、マスタメンテナンス、削除の取り消し、データ投入、データ抽出といった作業があり、これに対応する。なお、依頼のすべての作業が手順化されているわけではなく、ヘルプデスク要員自らがデータベース定義等の設計書を理解した上で、作業を実施する必要がある。また、一度実施した作業は同様の作業発生時に閲覧できるよう、手順書を作成すること。なお、データ投入にあたり、ツールの作成が必要になった場合は、作業依頼対応の中で対応すること。ただし、単にデータのメンテナンスにとどまらず、要件調整やアプリケーションの改修を伴うものについては、下記「保守業務の範囲定義」に基づき対応する。 ア　マスタメンテナンス 主に、下記の各種マスタの更新を行う。マスタは下記以外にも存在する為、必要に応じて更新を行う。 機構カレンダー，イベント・業務区分別イベント，審査期間目標，成分マスタ，調査区分マスタ，手数料コード，手数料，紙資料関連マスタ，企業向けパスワード発行，文書番号発番管理，承認番号発番管理，製造業・修理業許可番号発番管理，認定番号発番管理，汎用マスタ，汎用コード，CDISC 用語テーブル，SDTM ドメイン情報テーブル，Define-XML 情報管理テーブル，アクセス制御マスタテーブル，システム設定マスタテーブル，システム制御パラメータ イ　データ登録 承認原義、既承認画像などをスキャンし PDF 化した場合など、まとまったボリュームの文書ファイルを、文書管理機能上の適切な格納先へ、検索時に使用する文書属性を付与しつつ登録する。また、ファイルサーバにて管理している文書ファイル等についても、文書管理機能上の適切な格納先へ、検索時に使用する文書属性を付与しつつ登録する。文書属性を抽出するツールや文書ファイルを登録するためのツールは準備されているが、必要に応じて修正が必要となる事が想定される。なお、単に既存ツールを使用したデータ登録にとどまらず、投入先に係る要件調整やツールの改修を伴うものについては、下記「保守業務の範囲定義」に基づき対応する。 PMDA 担当者から提出される画像データ等（CD-R で年間 500 枚程度）を共有フォルダにコピーするとともに、データベースにインデクス情報を投入すること(専用プログラム使用)。また、データベース投入時にエラーが発生した場合は、その原因を調査し、軽微な誤

No.	名称	役割・概要
		りであれば修正し、再投入すること。作業内容はすべて作業ログとして蓄積し、PMDA 担当者に報告すること。また、依頼に応じて過去に投入された画像データの棚卸調査を実施し、調査結果を PMDA 担当者に報告すること。
1-9	⑨ アクセス管理	ア　ユーザ管理 申請電子データシステムおよび Pegasus は、PMDA のユーザに加えて、行政ユーザ（都道府県、厚生局、厚生労働省）、外部ユーザ（申請者）から利用される。これらのユーザのアカウント管理、アクセス権の管理を適切に行うことにより、申請者から預かる申請情報をはじめとした機密情報の機密性を確保する。 また、検証環境に作成されるアカウントや、ヘルプデスクの担当者に対して作成されるアカウントについても同様に管理を行う。 なお、年４回棚卸しを実施し、登録・更新・削除等行なうこと。 イ　OS ユーザ管理 サーバの機密性を確保するため、サーバ上で稼働するユーザについて適切に管理する。新規作成変更の際は、システム管理者からの承認をうけ作成する。また、年４回、作成されたユーザアカウントを棚卸しする。
1-10	⑩ 問合せ対応	平日の 9 時 30 分から 18 時 00 分（「3 作業の実施内容に関する事項（１）作業の内容 オ 作業期間等」に示した通り、支援業務の時間帯が変更された場合はその時間帯に従う）において、システムに関する PMDA 内の利用者、または厚労省ヘルプデスクからの問い合わせに対応すること。なお、厚労省ヘルプデスクからの問い合わせの内容としては、システム基盤に関する質問や、その発生事象がプログラムなどを解析しないとわからないような場合に問い合わせが発生することを想定している。問い合わせの方法は各システムにより異なるが、問い合わせ件数の合計は 10 件／日程度を想定する。また、質問、要望、障害等の区分によらず、応答記録を残すこと。問い合わせの多いものについては FAQ として情報抽出・整理を行い、月次で PMDA に報告すること。問い合わせは、システムの知識だけでは無く、医薬品・医療機器・体外診断薬・再生医療製品に係る以下の業務要件とシステム実装内容について理解している必要がある。以下知識を保有していない要員については受託者の費用負担で教育すること。 ・　申請受付業務 ・　承認審査業務 ・　添加物前例調査業務 ・　GCP/GPSP/GLP/GMP/QMS/GCTP 調査業務 ・　許可・認定・登録業務 ・　手数料管理業務 ・　施行業務 ・　台帳管理業務 ・　進捗・統計管理業務 ・　相談業務 ・　治験届及び治験調査業務 ・　本業務内に存在するサーバや通信機器等のログを横断的に解析する知識

<table>
<tr><th>No.</th><th>名称</th><th>役割・概要</th></tr>
<tr><td></td><td></td><td>
システム操作に関する質問については、適切な操作方法を回答すること。また、システムの動作不具合に関する問い合わせについては、問い合わせ内容を分析し、操作方法に起因する場合には適切な操作方法を回答すること。システム障害が疑われる場合には、状況について回答するとともに、障害対応手順に沿った対応を実施すること。システムの仕様に関する質問については、設計書およびプログラム解析を行い回答すること。
各システムの問い合わせ方法は「システム別問合せ元別問合せ方法対応表」のとおりであり、想定される頻度は以下の通り。

【システム別問合せ頻度】
・ Pegasus：月 120 件程度
・ 申請電子データシステム：月 80 件程度（パスワード初期化等の恒常的な対応も含む）
・ eCTD v3.2.2 ビューア：月 5 件程度
・ eCTD v4 関連システム：月 5 件程度
・ DWAP：月 10 件程度
・ 拠出金徴収管理システム：月 5 件程度（想定）
・ その他：月 5 件程度

＜システム別問合せ元別問合せ方法対応表＞
<table>
<tr><th rowspan="2">システム名</th><th colspan="3">問合せ元</th></tr>
<tr><th>PMDA 内役職員</th><th>厚生労働省,
都道府県,
地方厚生局</th><th>厚労省ヘルプデスク</th></tr>
<tr><td>Pegasus</td><td>メールおよび電話
（※2, 4）</td><td>（※3）</td><td>メール（※4）</td></tr>
<tr><td>申請電子データシステム</td><td>メールおよび電話
（※4）</td><td>－</td><td>メール（※4）</td></tr>
<tr><td>eCTD v3.2.2 ビューア</td><td>メールおよび電話
（※1, 4）</td><td>－</td><td>－</td></tr>
<tr><td>eCTD v4 関連システム</td><td>メールおよび電話
（※1, 4）</td><td>－</td><td>－</td></tr>
<tr><td>医療機器 Web 申請プラットフォーム</td><td>メールおよび電話
（※2, 4）</td><td>－</td><td>－</td></tr>
<tr><td>拠出金徴収管理システム</td><td>メールおよび電話
（※1, 4）</td><td>－</td><td>－</td></tr>
</table>
（※1） 基本的にはシステム管理者のみ。
（※2） 基本的には PMDA 内役職員全員となるが、DWAP は審査業務部の担当者、システム管理者のみ。
</td></tr>
</table>

No.	名称	役割・概要
		（※3） 厚生労働省、都道府県、厚生局からの問合せは、厚生労働省が調達する厚労省ヘルプデスクが窓口となるが、厚労省ヘルプデスクが解決できない場合は、エスカレーションされることがあるため、協力して解決にあたること。 （※4） 必要に応じて対面による相談も含む。
1-11	⑪ 情報提供	計画的なサーバ停止の連絡やアプリケーション改修後の連絡等、利用者に対し、システム運用に関する情報提供（情報のアップロード）を行うこと。また、情報提供は FD 申請ソフトのバージョンアップおよび対象モジュールの適用方法等についても情報提供の範囲とする。情報提供の手段は本システムのポータル及び共用 LAN 内イントラ（Sharepoint サーバ）とする。申請電子データシステムに関しては、PMDA 外部の利用者が多数存在するため、原則として遅くともシステム停止の 5 週間以上前に、外部向けのポータルサイト（申請電子データホームページ）のお知らせ掲載に加え、各利用者へのメール通知を実施すること。
1-12	⑫ 変更管理	課題管理や変更要求等によって、対象となるハードウェア、ソフトウェア等の資源への変更が発生する場合、その対応状況や進捗状況を管理すること。また、PMDA が変更を承認するための情報提供・説明、PMDA が実施する受入テストの実施支援を行うこと。
1-13	⑬ 構成管理	変更管理及びリリース管理に伴うハードウェア、ソフトウェア等の資源の版数管理、原本管理を行うこと。
1-14	⑭ 時刻同期管理	月 1 回、手順書等に基づき、各ハードウェアの時刻が正しく同期されていることを確認すること。
1-15	⑮ ログ抽出	任意のタイミング（月 2， 3 回程度）で依頼されるログ抽出において、指定された分析方法にて分析した結果を PMDA に提出すること。
1-16	⑯ 運用サービスレポート	月 1 回、状況把握、情報の棚卸しを行いサービスの品質維持を行うとともに、事業環境の変化やユーザからの要望を捉えてサービスの改善するため、運用サービスレポートを行う。ヘルプデスクは運用業務の改善案を提示し、手順書の追加／修正を行う。 運用サービスレポートでは、運用業務全般について報告を行う必要があるが、特に、サービスレベルの遵守状況、稼働統計（性能情報については、時系列（月別）の推移を含む）、運用状況（作業依頼件数、問合せ件数、発生障害内容など）、要員管理（研修状況、作業工数報告）、必要に応じた運用改善案についての報告が求められる。申請電子データシステムにおいては、上記に加え、システムの利用状況（アクセス件数、申請件数等）も報告すること。なお、様式については各システムで異なるが、PMDA の了解の上、様式を統合、変更等行なうことは問題ない。 また、報告に際し、インシデントレベルに応じて別様式に起票し報告する必要がある。記載方法、報告方法等については PMDA と協議の上決定すること。
1-17	⑰ 証明書類の更新	基本的には各サーバ等に年 1 回、サーバ証明書等を更新すること。サーバ証明書本体は、別途 PMDA が調達しているため、各サーバ等への適用作業のみ行なうこと。サーバ証明書を適用する対象サーバ等は 10 台程度で、コードサイニング証明書を適用する対象サーバは 5 台程度となる。
1-18	⑱ 統計処理	PMDA 担当者が提示した統計表の作成業務、及び、PMDA 担当者から依頼された業務上急遽必要となったデータの抽出、集計業務。統計表を作成するにあたり、過去データの正確性を確保するため、各システム間の不整合データが確認された場合、不整合データの原因の調

No.	名称	役割・概要
		査・分析を行い、不整合データの修正箇所の特定、報告を行うとともに、PMDA 担当者の指示の下、修正、削除の実施、確認、記録業務への即時対応を行う。 ア　統計処理業務 全ての統計処理業務は、Pegasus 等の各機能を利用して抽出したデータとツールにより各テーブルから集計したデータ、旧法については仮想環境からツールにより集計したデータを利用して行う。集計に際しては、Pegasus 等の運用前の統計方法を確認し、同じ集計を実施すること。なお、すべての作業が手順化、ツール化されているわけではなく、集計した結果には、何らかの理由により不整合データも含まれる為、原因の調査・分析等実施、修正箇所の特定、報告をヘルプデスク要員自らがデータベース定義等の設計書を理解した上で、手作業で実施する必要がある。また、PMDA 職員の求めに応じて、統計処理業務を実施するに当たって新たに必要となるツールの作成または既存ツールの改修を行うと共に、作業が継続的に実施出来るよう、手順書を作成・修正すること。 ア－１　下記に示す種類の統計処理業務を実施すること。 ● 前年度集計（確定版）：令和 8 年 4 月下旬の PMDA 担当者が指示した日に、令和 7 年 4 月から令和 8 年 3 月末までのデータを抽出し、令和 8 年 4 月末日頃を目処に集計報告を行う。 ● 毎月集計：毎月、PMDA 担当者が指示した日に、令和 7 年 4 月 1 日（令和 8 年度の場合は令和 8 年 4 月 1 日）から前月末までのデータを抽出し、毎月 18～20 日頃に集計報告を行う。 ● 前年集計：令和 8 年 1 月（令和 8 年度の場合は令和 9 年 1 月）の PMDA 担当者が指示した日に、令和 7 年 1 月から令和 7 年 12 月（令和 8 年度の場合は令和 8 年 1 月から令和 8 年 12 月）までのデータを抽出し、令和 8 年 1 月 20 日（令和 8 年度の場合は令和 9 年 1 月 20 日）頃を目処に集計報告を行う。 ア－２　集計結果を反映する統計表については、急遽変更する場合があるので PMDA 担当者と相談の上対応すること。 ア－３　上記、統計表の他、月初めに抽出したデータにおいて、新医薬品及び新医療機器の関係については速報として月の 8 日前後までに PMDA 担当者に報告すること。 ア－４　統計表以外に PMDA 担当者より業務上急遽必要となった統計表に基づいたデータの抽出、分析、集計について即時に支援（依頼があってから作成完了までを 1 ～ 2 日程度）すること。 ア－５　また、統計表を作成するにあたり、過去データの正確性を確保するため、各システム間の不整合データが確認された場合、不整合データの原因の調査・分析を行い、不整合データの修正箇所の特定、報告を行うとともに、PMDA 担当者の指示のもと、修正、削除の実施、確認、記録作成等の即時対応を行うこと。なお、この場合においても再集計を含む統計表の提出は期限内での実施が必要となる。 ア－６　集計業務に使用したツール及びプログラムを PMDA 担当者に必要に応じ開示し簡易にデータ抽出をできるツールを作成し、マニュアルも作成すること。 ア－７　集計業務に使用したツール及びプログラム等においても、本紙「７（１）知的財産権の帰属」に該当するものとする。 ※統計表フォーマットについては、閲覧資料 13「統計処理業務関連資料」を参照。

No.	名称	役割・概要
		イ　仕掛審査等費用業務 イ－１　毎月月末を期限とし、Pegasus 審査系システムよりデータを抽出し、部門別に必要データのみを記載した、翌月の審査時間入力用シートを作成すること。（閲覧資料 13「統計処理業務関連資料」参照） イ－２　毎月月末を期限とし、前月分の個人ごとの審査時間入力シートを部門毎の審査時間集計表としてとりまとめを行い、承認を得ること イ－３　９月末、１１月末、３月末については、当年度中の審査時間集計表を作成するとともに、部門毎に作成した審査時間集計表を品目ごととした品目別審査時間集計表を作成すること。 なお、品目別審査時間集計表を作成する際に、PMDA 担当者が指定するデータを Pegasus システムより抽出し、品目別審査時間集計表に付加すること。 イ－４　審査時間入力用シート、各種集計表は PMDA の指示があった場合には、修正等を行うこと。 イ－５　その他については、閲覧資料 13「統計処理業務関連資料」参照 ウ　GMP 等調査実績集計業務 ウ－１「GMP 等調査実績集計業務手順書」に従い、下記に示す時期に GMP 調査関連情報集積システム（まとまるくん)よりデータを抽出し、予め定められた集計表フォーマットに結果を転記すること。 ウ－２　下記に示す種類の統計処理業務を実施すること。 ● 前年度集計：令和８年４月の PMDA 担当者が指示した日に、各年４月から翌年３月末までのデータを抽出し、各年の４月２０日頃を目処に集計報告を行う。 ● 半期集計：令和７年１１月および令和８年１１月の総合機構担当者が指示した日に、各年４月から１０月末までのデータを抽出し、各年１１月７日頃を目処に集計報告を行う。 ウ－３　集計結果を反映する表については、急遽変更する場合があるので PMDA 担当者と相談の上対応すること。 ウ－４　上記集計以外に PMDA 担当者より業務上急遽必要となったデータの抽出、集計について即時に支援（依頼があってから作成完了までを１～２日程度）すること。 エ　医療機器承認品目一覧作成業務 エ－１　手順書に従い Pegasus システムから医療機器の集計データを抽出し、予め定められた 2 種類の集計表フォーマットに結果を転記すること。 エ－２　本業務を実施する時期は、四半期に一度の年 4 回を想定している。なお、年度当たり 2 回目以降の集計は、前回の結果に追加する形で集計すること。 エ－３　集計結果を反映する表については、急遽変更する場合があるので PMDA 担当者と相談の上対応すること。 エ－４　上記集計以外に PMDA 担当者より業務上急遽必要となったデータの抽出、集計について即時に支援（依頼があってから作成完了までを１～２日程度）すること。

No.	名称	役割・概要
1-19	⑲ 情報資産棚卸しおよびリスク評価支援対応	本運用保守業務内の情報システムについて、システムが保有している情報資産の洗い出しおよびリスク評価を行なうにあたり必要となる情報等を指定された様式にて提供すること。対象となる情報資産はシステムのデータベース内にある全テーブル、ファイルサーバに登録されている全文書ファイル、システムから出力された帳票やその他紙情報等多岐にわたる。それぞれについて、システム的な目的、業務的な目的、運用での使用方法を整理する必要があるため、高いレベルでのシステム知識、業務知識が求められる。なお、詳細については PMDA 担当者と相談の上決定すること。
1-20	⑳ 拠出金徴収管理システムにおける期末期首処理の支援	拠出金徴収管理システムでは業者台帳や品目台帳等、一部のマスタデータを年度ごとに管理しており、期末から期首にかけて次年度の業務に向けたマスタデータを整備する業務が発生する。これにあたり、業許可情報や承認品目の取得、取込み等、PMDA 内役職員からの作業依頼を踏まえて作業を実施すること。 本運用に係る具体的な実施時期や作業手順、ならびに作業の効率化に資するツールの作成については PMDA 内役職員と相談の上決定し、進めること。
1-21	㉑ その他の作業	その他、運用にあたり実施すべき作業として下記に例示される業務を実施する。実施タイミングや管理方法は、ヘルプデスクとシステム管理者で協議し決定する必要がある。 1　相談月初受付日マスタ更新 ・　実施タイミング 年１回（原課より情報入手次第。数年分をまとめて処理することも可） ・　実施方法・概要 対面助言等申込み Web 受付機能（バッチ処理）の稼働日情報を年月日の形式でシステムが保持している。原課より Web 申し込みを行う予定日を受け取り、ヘルプデスクにて汎用マスタを更新する。 2　部会分科会判定マスタ更新 ・　実施タイミング 年１回（原課より情報入手次第。数年分をまとめて処理することも可） ・　実施方法・概要 部会・分科会の開催年月をシステムが保持している。「SSNSS02-新医薬品の審査期間集計（承認）」の機能のみで利用される。原課より部会・分科会の開催年月を受け取り、ヘルプデスクにて汎用マスタを更新する。 3　対面助言年度計画マスタ更新 ・　実施タイミング 年１回（原課より情報入手次第。数年分をまとめて処理することも可） ・　実施方法・概要 対面助言の記録確定までの年度ごとの達成目標をシステムに保持している。対面助言の年度計画が決定次第、原課より情報を受け取り、ヘルプデスクにて汎用マスタを更新する。 4　目標審査期間マスタ更新 ・　実施タイミング 年１回（原課より情報入手次第。数年分をまとめて処理することも可） ・　実施方法・概要 承認審査における審査期間の目標値として公表されている「審査期間目標値」を

No.	名称	役割・概要
		システムに保持している。承認審査の目標審査期間の情報が決定次第、原課より情報を受け取り、ヘルプデスクにて汎用マスタを更新する。 5　旧法データ月次移行 ・　実施タイミング 月１回 ・　実施方法・概要 運用手順書に記載。（旧法データ月次移行運用手順書） 6　システムメール不達対応 ・　実施タイミング 不定期（発生都度） ・　実施方法・概要 運用手順書に記載。（システムメールの不達対応手順書） 7　外部ポータル不正ログイン履歴の確認 ・　実施タイミング 不定期（発生都度） ・　実施方法・概要 運用手順書に記載。（外部ポータル不正ログイン履歴の確認手順書） 8　SharePoint Server コンテンツ DB のサイズ確認 ・　実施タイミング 月１回 ・　実施方法・概要 SharePoint Server コンテンツ DB が肥大すると、文書管理機能の性能劣化が懸念される。(1 つのコンテンツ DB あたり 200GB が性能劣化の起きる目安。) SharePoint Server の管理画面よりサイズの確認を行う。 9　制度変更等による対面助言画面の項目追加等 ・　実施タイミング 年 10 回程度 ・　実施方法・概要 対面助言画面は設定ファイルを機能で読み込み検索画面、登録画面を動的に作成している。そのため対面助言画面は設定ファイルを更新することで画面の追加・更新・削除、および項目の追加・更新・削除が行なえる。制度変更等により、相談区分の追加や相談定義の変更等必要がある場合、PMDA の求めに応じて画面の追加・削除等を行うこと。また、既存の画面に項目の追加や削除等必要がある場合、PMDA の求めに応じて項目の追加や削除等を行なうこと。なお、設定ファイルの設定方法についてはマニュアルに全て記載されているわけではないので、全体として約 65 種類の対面助言画面の設定ファイルに対し、設定すべき内容（35 項目）それぞれの目的、設定方法、設定による動作等を運用マニュアル、各種設計書、プログラムで理解したうえで対応する必要がある。また、対面助言の申請に伴い設定ファイル自体を新たに作成することが必要となる場合もある。プログラム修正が必要な要望については、下記「保守業務の範囲定義」に基づき、PMDA と相談の上対応すること。データ修正が必要なものについては、PMDA から修正対象を明示

No.	名称	役割・概要
		できる場合は、無償で対応し、要件調整が必要なものは下記「保守業務の範囲定義」において、PMDA と相談の上対応すること。 １０ AccessDB から Pegasus データ登録 ・ 実施タイミング 週１回 ・ 実施方法・概要 軽微変更届について一部 AccessDB にデータを登録しているものがある。その結果を Pegasus にデータ登録すること。Pegasus へのデータ登録は基本的にツールを利用することで実施可能ではあるが、ログ等確認し、問題なく実施できていることも確認すること。 １１データ抽出用 Access のメンテナンス ・ 実施タイミング 年４回程度 ・ 実施方法・概要 業務効率化のために作成したデータ抽出用の Access であり、基本的な構造としては、Pegasus からデータを抽出して Access 上に画面表示をし、申請ごとに Excel の帳票を出力できるというものである。また、ジョブ管理によって、毎夜自動的にデータ更新および Excel 帳票の出力を行っている。 本機能のメンテナンスとは、データ抽出対象の修正や Excel のテンプレートを更新した際の位置修正やデータ抽出対象が増えたことなどによるデータの配置等を行うものである。現時点で必要なデータはそろっているものの、業務を行う上で必要なデータが増えることを見越し、年 4 回程度の修正を依頼するものである。 １２ eCTD v4 CV（CT）更新対応 ・ 実施タイミング 年４回程度 ・ 実施方法・概要 申請電子データシステムの SDTM と ADaM の terminology バージョンを追加更新する際には、合わせて以下を実施すること。 ● eCTD v4 コントロールド・ボキャブラリ（以下、「CV」という。）の更新 ● eCTD v4 審査システムの CV 関連テーブル更新作業 ● 設定データ更新パッケージファイルの出力（CV 関連テーブル更新後に「バリデーションルール更新ファイル出力」機能から実施） 当該 terminology バージョン追加更新前の最新 CV は、「eCTD v4 国内コードリスト & Genericode 一覧」（https://www.pmda.go.jp/int-activities/int-harmony/ich/0104.html）ページにある公開日が最新の Version の掲載物から解凍/取得できる Excel 形式のファイルである。また、CV 関連テーブルの更新作業には、当該更新内容が反映された genericode ファイルを eCTD v4 審査システムの「CV 取込管理」機能から取込む必要がある。したがって CV 更新後、公開用 genericode ファイルを作成すること。なお公開用 genericode ファイルの作成にあたっては、PMDA が作成したツールを利用すること

No.	名称	役割・概要
		ができる。（作業者がより利用しやすいように当該ツールを改変することは差し支えない。ただし、改変した場合には取込む前に出力結果を PMDA 担当者に確認すること。）取込みにあたり genericode ファイルごとに有効期間を設定する必要があるため、取込前に PMDA 担当者に確認すること。作業完了後、更新した CV 及び作成した genericode ファイル、設定データ更新パッケージファイルは PMDA 担当者に提示すること。eCTD v4 検証ツール用の CV ファイルや、genericode ファイルの公開作業（HP 掲載作業）は、本業務の対象外とする。 １３オンライン専門協議対応 ・ 実施タイミング 月 10 回程度 ・ 実施方法・概要 外部専門委員がオンラインで担当品目の申請資料を閲覧するための環境に対し、PMDA 職員からの依頼によって AD アカウントの管理やフォルダへのアクセス権設定、ショートカットの作成などを実施する。 １４拠出金徴収管理業務及び審査手数料等回収業務における会計システム連携不具合対応 ・ 実施タイミング 月 5 回程度 ・ 実施方法・概要 拠出金徴収管理業務及び審査手数料等回収業務においては、業務プロセスの中で Pegasus から会計システムに CSV 等の形式で債権等のデータを連携し、会計システムにて債権と入金とを突合、消込処理を行い、その結果のデータを CSV 等の形式で受領し、当該データを Pegasus 取り込むという処理が発生する。これらの一連の処理の中で何かしらの不具合（例：会計連携用のファイルが生成されない、消込結果のファイルが取り込めない等）が発生した場合、PMDA 内役職員にエスカレーションをし、対応方針について合意した上で対応すること。 その他、会計連携に係る作業依頼（例：任意のタイミングでの会計連携、会計連携の差し止め等）について、PMDA 内役職員からの作業依頼を踏まえて対応すること。

保守業務の範囲定義

<table>
<tr><th>No.</th><th>名称</th><th>役割・概要</th></tr>
<tr><td>2-1</td><td>① アプリケーション保守</td><td>
ア　作業概要
各システムで発するアプリケーション不具合等について、PMDA と協議の上、必要な修正を実施すること。また、業務の効率化、利便性の向上に資するために、PMDA の指示のもと、下記の作業を実施する。その際、必要な設計書と操作手順書の改訂・作成も併せて実施すること。（年間 100 人月程度（※）までの作業とする。なお、この人月は影響調査や実装などの実作業で計上することの出来る工数であり、仕様理解や打合せ等で PMDA に移動する時間は含めないものとする。仕様理解や打合せ等で PMDA に移動する時間については自らが負担すること。）原則、本作業は専任の要員で実施することとし、PMDA に常勤するヘルプデスク要員は本作業を実施しないこと。ただし、ヘルプデスク業務に支障がない場合においては、この限りではない。
イ　生産性
工数は PMDA の業務や医薬品医療機器等法に精通したエンジニアの生産性で算出した数値である。受託者は自社のノウハウ・スキル等をよく検討し、問題なく業務遂行可能な体制を提案すること。PMDA が著しく低い生産性と判断した場合は、上記工数への計上は認めず、追加の作業を依頼することがある。また、いかなる場合も契約変更は行わない。
ウ　工数内訳
令和 8 年度の総工数は 140 人月、令和 7 年度は 7 月からのため 90 人月とする。なお、各システムの大まかな工数内訳としては、以下のとおりであるが、状況に応じて協議の上、配分を見直すことがある。また、あるシステムの工数超過分を本業務範囲内の別システムの工数として使用する場合もある。
<table>
<tr><th>対象システム</th><th>令和 7 年度</th><th>令和 8 年度</th></tr>
<tr><td>Pegasus</td><td>35 人月</td><td>54 人月</td></tr>
<tr><td>申請電子データシステム</td><td>18 人月</td><td>32 人月</td></tr>
<tr><td>DWAP</td><td>2 人月</td><td>4 人月</td></tr>
<tr><td>eCTD v3.2.2 ビューア</td><td>2 人月</td><td>4 人月</td></tr>
<tr><td>eCTD v4 関連システム</td><td>9 人月</td><td>13 人月</td></tr>
<tr><td>拠出金徴収管理システム</td><td>24 人月</td><td>33 人月</td></tr>
<tr><td>合計</td><td>90 人月</td><td>140 人月</td></tr>
</table>
※1 人月は 20 人日とし、1 人日は 8 時間とする。
エ　作業詳細
アプリケーション保守で対応する内容を以下に記す。ただし、下記以外においても工数をかけることで対応できる案件があれば対応すること。
・　障害対応などに起因する不具合修正
・　クライアント PC のソフトウェア更新(Microsoft Office のアップグレード等)に起因する不具合修正
・　軽微な改修
・　設定変更（ハードウェア、OS、ミドルウェア）、ジョブスケジュールの修正
</td></tr>
</table>

No.	名称	役割・概要
		・　静的画面の更新 ・　画面・帳票レイアウトの変更、検索条件の修正 ・　小規模ツールの作成 ・　要件調整が必要なデータ投入 ・　「マイリスト」、「素データ出力」の作成・修正、登録 軽微な改修は、要望として分類された問合せ一覧を対象として実施することになるが、この一覧に具体的な改修内容が記載されているわけではなく、修正すべき機能や範囲を受託者が設計書及びプログラムソースを理解した上で、各部署の担当者に直接要件の確認を行い、実現方法の検討、他部署との調整、影響機能の洗い出しを含めて主体的に実施すること。また、当年度新たに発生した要望も対象とすること。 オ　作業実施場所 開発に必要な作業場所・機材・開発環境は受託者の費用負担で業務が開始される日までに利用出来る状態を準備すること。 カ　開発環境 保守業務を目的として使用する開発環境の構築は、受託者自身で受託者の拠点内に行うこと。構築に必要とする各種ソフトウェアのライセンスは、受託者の費用負担で業務が開始される令和７年７月１日までに準備すること。構築に必要となるソフトウェアは閲覧資料に含まれるソフトウェア一覧を参照し、受託者で判断すること。構築に必要な設計書一式、プログラム一式、データベース定義一式は貸与する。なお、必要に応じて、過去の開発プロジェクトで納品された開発環境の仮想イメージを貸与することは可能であるが、現行本番環境と完全に一致するものではないため、差分の構築は受託者自身で行うこと。また、貸与する仮想イメージに有償ソフトウェアが含まれるが、このソフトウェアをそのまま使用する場合は、受託者が各ソフトウェアのライセンスを購入すること。また、開発環境用のデータは、一部のマスタ系データを除き、受託者で生成すること。 キ　作業手順 アプリケーション保守でこれらの作業は、事前に取り決めたプロセスに従って実施し、課題管理、変更管理を行う必要がある。構成管理、リリース、ビルドについては所定の手順書に従って作業を行う。また、これらの作業の検証を行うための検証環境について継続的に整備を行う必要がある。なお、アプリケーションの改修においては、非改修部分を含めたリグレッションテストを実施し本業務における対象のシステム全体（周辺システム含む）としての動作保証をおこなうこと。改修によって非改修部分に影響を及ぼした場合はそれも正すこと。 ク　責任範囲 アプリケーション保守また、改修部分のみならず、影響調査漏れ等を起因として非改修部分に影響を及ぼした場合も含め、改修が影響する全てのシステム範囲において契約不適合対応を契約終了後から１年間無償で実施とすること。なお、改修や契約不適合対応の実施においてアプリケーション開発業者の協力が必要な場合は、委託可否の確認・調整・契約等を受託者の責任により速やかに実施し、費用負担も行うこと。PMDA は調整、費用負担等は行わない。

No.	名称	役割・概要
2-2	② アップデート	ハードウェア、OS、ミドルウェア等の資源にかかるセキュリティパッチ及び最新アップデートプログラムの適用について、緊急性及び各システムへの影響を情報処理技術者試験（情報セキュリティスペシャリスト）の資格を有する者、もしくは情報処理安全確保支援士の登録を受けた者が調査分析し、PMDA へ適用可否の提案を行うこと。その提案を元に PMDA と協議の上、検証テストを実施の上で本番環境に反映させること。Microsoft 等が公開するセキュリティパッチについては、インターネット接している通信機器およびサーバについては少なくとも３ヶ月に１度はパッチ適用するが、インターネットに接していない内部向けの通信機器、サーバについては半期に一度パッチ適用を行うこと。なお、緊急性の高いパッチがある場合は随時対応する。その他のベンダなどから緊急で展開されるパッチがあれば随時、適用する。実施タイミングは通常夜間又は休日に行なうこと。なお、本アップデート作業に伴い、アプリケーション改修が必要になる場合は PMDA に実施可否の指示を仰ぐこと。アプリケーション改修が伴うアップデート以外にかかる費用は受託者の負担において実施すること。
2-3	③ 試験データバリデーションルールの変更に伴うシステム変更	PMDA からの依頼があった場合、保守手順書に基づき、バリデーションルールの事前検証、変更作業、動作確認を実施すること。なお、バリデーションルールの変更により、アプリケーションの改修が必要な場合は、「①アプリケーション保守」において対応し、バリデーションルールの変更により発生する費用は受託者の負担において実施すること。

その他業務の範囲定義

No.	名称	役割・概要
3-1	① 審査知識データベース維持・管理業務	原則として１名の要員が以下の業務に従事して対応すること。 ア　PMDA が作成した審査報告書等の審査知識をデータベース化する業務 ● PMDA 職員の指示に従って審査報告書等の原資料・情報の収集状況を記録した資料を随時アップデートし、所定の共有フォルダに保存する。四半期に一度、一斉提出依頼を行うため、少なくとも年度毎に４回分のアップデート版を作成・バックアップする ● 原資料・情報を基にデータベースの内容を随時アップデートする他、少なくとも年度毎に二回のバックアップ作成を行う。データベースの形式や構成を変更する場合は、その前後でバックアップを必ず作成する。 ● 上記の手順書を令和５年度中に作成する。その後、必要に応じて手順書を更新する。 イ　将来的な審査系システムへの統合を視野に入れた、当該データベースを作成・活用するためのデータベース管理ツール（プログラム）の作成・維持・管理（改修等を含む） ● 利用者への意見聴取を年度毎に１回程度実施し、必要に応じてデータベース管理ツール（利用者用プログラム・データ入力用プログラム等）の新規作成または改訂を行う。作成や改訂の際は、作業の記録を残すこと。 ● 当該ツールの仕様・内容（構成やコード等）を説明する資料を作成すること。作成する資料は、画面一覧、機能一覧、処理概要一覧、テーブル一覧とし、その他 PMDA 職員と協議の上、必要に応じて補足資料を作成する。

No.	名称	役割・概要
		● 当該ツールの使用方法を説明する資料を令和 5 年度中に作成する。その後、必要に応じて資料を更新すること。
3-2	② 令和 7,8 年度実施予定審査系システム改修業務への対応	令和 7,8 年度中に開始および終了する審査系システムへの改修業務の実施を予定している。 その開発業務を担当する業者と密に連携し、必要な助言を行うとともに最新の設計書類や各種設定、改修内容、開発に必要なデータの提供、各システムに係る技術的な質疑応答、リリース予定の把握等、本業務の運用保守対象となるシステムに関係する必要な情報共有および対応を適宜実施すること。なお、本対応は、上記「保守業務の範囲定義　①アプリケーション保守」に記載する作業工数を使用せずに対応すること。 また、改修業務で改修されたプログラムを PMDA 担当者と時期を協議の上で受領し、本業務で改修したプログラムとマージし、本番環境へリリースする作業を行うこと。マージ作業の工数は、「2-1 ①アプリケーション保守」に記載する作業工数とは別に、各年度 10 人月を見込むものとし、その当時において必要工数が超過する見込みがある場合は、PMDA と相談の上、保守工数を使用して対応すること。

目次

■別紙11　その他の要件

アクセシビリティ要件

目次に戻る

No.	アクセシビリティ分類	アクセシビリティ要件	補足
1	全体	電子政府ユーザビリティガイドライン https://cio.go.jp/node/1980	最新のガイドラインを参照すること
2	全体	JIS X 8341-3	適合レベルAAに準拠すること

目次に戻る

システムの設計・開発等に際しては、受注者は、PMDAと調整の上、必要な対策を講じること。なお、情報セキュリティ対策を講じる範囲は本システム全体とする。主な対策例を下表に示す。

No.	情報セキュリティ対策	対策に係る要件	補足
1	コンピュータウイルス対策	コンピュータウイルス対策基準（平成12年12月28日（通商産業省告示 第952号））に準じた対策を講じること。	
2	ボット対策	ボットに感染したコンピュータからのサイバー攻撃等を迅速かつ効果的に停止させるための対策を考慮すること。	
3	不正アクセス対策	ウェブサイトに係る機能等に関しては、クロスサイト・スクリプティングやSQLインジェクション等の脆弱性を狙った攻撃に対する対策を講じること。	
4	脆弱性対策	・ソフトウェア等脆弱性関連情報取扱基準（平成16年7月7日（経済産業省告示 第235号））に準じた対策を講じること。 ・PMDAの指示に従って脆弱性対策を行うこと。	
5	監査証跡（ログ管理）	・オンライン処理について、利用者ID、IPアドレス、利用機能、アクセス日時等について、ログが取得出来ること。 ・ログの収集及び一元管理が可能であること。ログファイルは一定期間ハードディスク上に保存し、それを超えた分については、外部可搬媒体にて保存させること。 ・定められた場所に定められた保存期間のログが保存されていることを年次検証すること。	
6	特権ID管理	・PMDAの指示に従って特権IDの管理（一覧の作成、棚卸、払い出しから返却までの管理、履歴管理）を行うこと。	
7	ユーザーIDの棚卸	・ユーザーIDの棚卸を支援すること。 ・PMDAの指示に従て不要IDの削除、不要権限の剥奪、パスワードの再設定を行うこと。	
8	パスワード管理	・PMDAの指示に従ってパスワード・ルールの設定と運用を行うこと。 ・一般利用者の他、サーバー、ネットワーク機器、業務システム、クラウドサービスの特権IDを含むパスワードを持つ全てを対象とする。 ・機器及びサービスの特性上、もしくは、運用手順の変更が必要となるためパスワード・ルールに準拠できない場合、PMDAと協議のうえ、代替策を講じること。	

No.	情報セキュリティ対策	対策に係る要件	補足
9	その他	・実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。 ・電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。 ・法人外の利用者その他のプライバシーに係る情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。	

目次に戻る

プログラム改修内容の特性に照らし合わせて下表のテストの内、実施するテストをPMDAと協議のうえで決定すること。

No.	テストの種類	テストの目的、内容	テスト環境	テストデータ	補足
1	単体・結合テスト	ソフトウェアをほかのソフトウェアと結合する前に単体でその完全性を評価する。また、それらの結合テスト・評価を行う。			
2	機能テスト	アプリケーションの各機能が実行するタスクが、仕様書・ユーザガイド・要求仕様書・設計文書に違反する動作をしていないかを確認する。 （TOFT：Task-Oriented Functional Test）			
3	強制エラーテスト	プログラムを強制的にエラーにするよう設計された異常系テスト 境界値テスト 極端な入力データに対するプログラムの応答を確認する。 （FET：Force-Error Test）			
4	システムレベルテスト	システム全体を通して動作させ、正常に機能するかを確認する。			
5	現実のユーザレベルテスト	ユーザがプログラムに対して行うであろうことを予測してテストする。			
6	探索型テスト	問題の「起こりそうな」場所に焦点をしぼってテストする。			
7	負荷／ボリュームテスト	プログラムが大量のデータ／計算／処理をどのように扱うかをテストする。			
8	ストレステスト	限られたリソースのもとでプログラムを動作させる。			
9	パフォーマンステスト	ユーザが許容できるシステム性能を維持できるかどうかをテストする。			
10	APIテスト	バグ修正後に、それが確実に修正されているかとともに、新たなバグが発生していないかをテストする。			
11	ドキュメントテスト	リファレンスガイドやユーザガイドが正しく記述されているかをテストする。			
12	ユーティリティ、ツール、その他付属品のテスト	システムに付属するもののテスト、インストール／アンインストールテスト、インストーラのテスト、READMEやアイコンの確認、インストールした機能が正常に動作するかをテストする。			
13	フェイルオーバーテスト	システムレベルのエラー処理やリカバリプロセスをテストする。			
14	アベイラビリティテスト	システムやコンポーネントが動作可能でアクセス可能な状態となるまでをテストする。			
15	信頼性テスト	システムが一定時間の間連続で操作可能かをテストする。			
16	ユーザインタフェイステスト	使いやすさや見た目の評価、UIが仕様通りに動作するかをテストする。			
17	ユーザビリティテスト	使いやすさやユーザの満足度をはかる情報を収集する等、場合によっては、外部の協力者の評価も交えてテストする。			
18	セキュリティテスト	脆弱性／情報洩れ等がないかをテストする。			

移行対象データ

目次に戻る

小規模改修でデータ移行が必要となった場合に定めるものとする。

No.	移行元	移行対象データ	件数	提供方法	補足
1					
2					

教育対象者の範囲、教育方法

目次に戻る

要員は、運用開始に先立って、以下の技能を習得しなければならない。また、PMDAを通じてマニュアル等を提供するので、運用開始までに要員への使用方法や薬機法等に関する教育を十分に行っておくこと。

No.	教育対象者の範囲	教育の内容	教育の実施時期	教育の方法	教材	教育対象者数	補足
1	本業務に従事する要員	個人情報保護・プライバシー保護に関する教育	参画前	受注者における社内教育	受注者が用意する教材	本業務に従事する要員数	社内教育制度を有し、業務に従事する要員に対し教育を実施していること。
2		守秘義務に関する教育					
3		情報セキュリティに関する教育					
4		効率的で高い顧客満足度を得るための業務実施方法に関する教育					要員が本業務に従事するに当たっては必要な応答要領を整備し、それに沿った応答を可能とするために必要な訓練を行うこと。
5		現行の薬機法の概要に関する教育					
6		本システムのデータ構造の概要に関する教育					
7		本システムを構成するハードウェア及びソフトウェアの基礎知識および本システムを構成する機器及び関連ソフトの基本操作に関する教育					
9		緊急対応に関する教育・訓練					
10		効率的で高い顧客満足度を得るための業務実施方法に関する教育	参画後	受注者における社内教育	受注者が用意する教材	本業務に従事する要員数	継続的な応答履歴等の分析（類型的又は特に重要と認められる質疑応答事例の抽出等の作業を含む。）を通じて応答要領の見直しを行い、改善意見を総合機構に提出すること。
11		一次応答の指導					必要に応じて上位の者がモニタリングを実施し、それに基づいて随時、必要な指導を行うこと。
12	PMDA職員	運用手順	システム変更本番リリース前	研修	納入成果物に示す各種マニュアル		調達仕様書の成果物に示す、本システムの運用支援に関する各種ドキュメント類を作成・改訂（本システムの保有する各種マニュアル類について、本業務の影響箇所を抽出の上、改訂を行うこと。）するとともに、利用者の人数や業務に応じて、運用手順に係る教育・研修等をPMDA等に行うこと。教育・研修の内容、日程、回数等の詳細については、PMDAと協議の上決定すること。

別紙１２

システム運用管理基準

2020 年 12 月
独立行政法人　医薬品医療機器総合機構

【資料の見方】
- ✧ システム運用業務を「１３の領域」に分けている。
  それぞれの業務プロセスは、標準化対象外。各情報システムの体制･特性･リスク等により、最適なプロセスを設計し、運用する。
- ✧ システム運用の標準化（要件）は、システム運用者（委託先）から当機構への報告書式（情報提供も含む）を統一し、各システムの運用状況を定期的に収集して、全体状況の把握と情報共有等を可能とすることにある。
  - 当資料においては「標準化」のタイトル等にて報告を記載している。
  - 標準化（要件）は、「報告書式を統一する領域」と「報告内容を統一（書式任意）」の 2 タイプに分かれる。
  - 「報告書式を統一する領域」は、インシデント管理、変更管理、構成管理、脆弱性管理、アクセス権管理の領域となっている。

改訂履歴

改定日	改定理由
2018 年 6 月 8 日	初版発行
2018 年 7 月 20 日	情報セキュリティ遵守状況報告内容を追記
2018 年 9 月 10 日	脆弱性管理を追記
2019 年 8 月 15 日	2. システム運用管理業務の概要に「【参考】システム運用管理業務の全体像」を追加 4.5 構成管理　最新情報を PMDA に報告する標準書式を定義 4.9 脆弱性管理　管理状況を報告する PMDA 標準書式を定義
2019 年 12 月 20 日	4.7 バックアップと回復管理　バックアップデータの保管方法を追加
2020 年 12 月 10 日	4.6 運行管理　ログ取得・保存、イベント検知対応の報告を標準化 4.9 脆弱性管理　管理要件を追加 4.10 アクセス管理　アカウント管理要件の追加、アカウント台帳作成と棚卸を標準化項目に追記

1. はじめに

1．1　目的

独立行政法人医薬品医療機器総合 PMDA（Pharmaceuticals and Medical Devices Agency）（以下、「PMDA」という。）が調達し、又は、開発した情報システムの運用管理を確実かつ円滑に行い、利用者が要求するサービス品質を、安定的、継続的かつ効率的に提供するために、情報システムの運用管理に関する業務内容を明確化・標準化するために定めるものである。

1．2　対象範囲

PMDA が調達し、又は開発・構築した全ての情報システムの運用保守を担当する組織（情報システムの運用保守業務を外部委託する場合における委託先事業者を含む）に適用する。

1．3　適用の考え方

システム運用管理業務は、既に開発・構築しサービスイン（本番稼動）している情報システムの運用・保守業務の実行と管理に係る業務を対象とする。

情報システムの運用・保守を外部委託する場合は、本資料をもとに委託先事業者において、当該情報システムの種類・規模・用途を踏まえた適切な運用手順を策定のうえ、運用サービスを提供するものとする。

1．4　用語の定義

本基準で使用する用語は情報システムの「ITIL（IT Infrastructure Library）」のガイドラインを踏まえた運用プロセス定義に準拠するものとする。

1．5　準拠および関連文書

上位規程　：「情報セキュリティポリシー」
関連文書　：「情報システム管理利用規程」

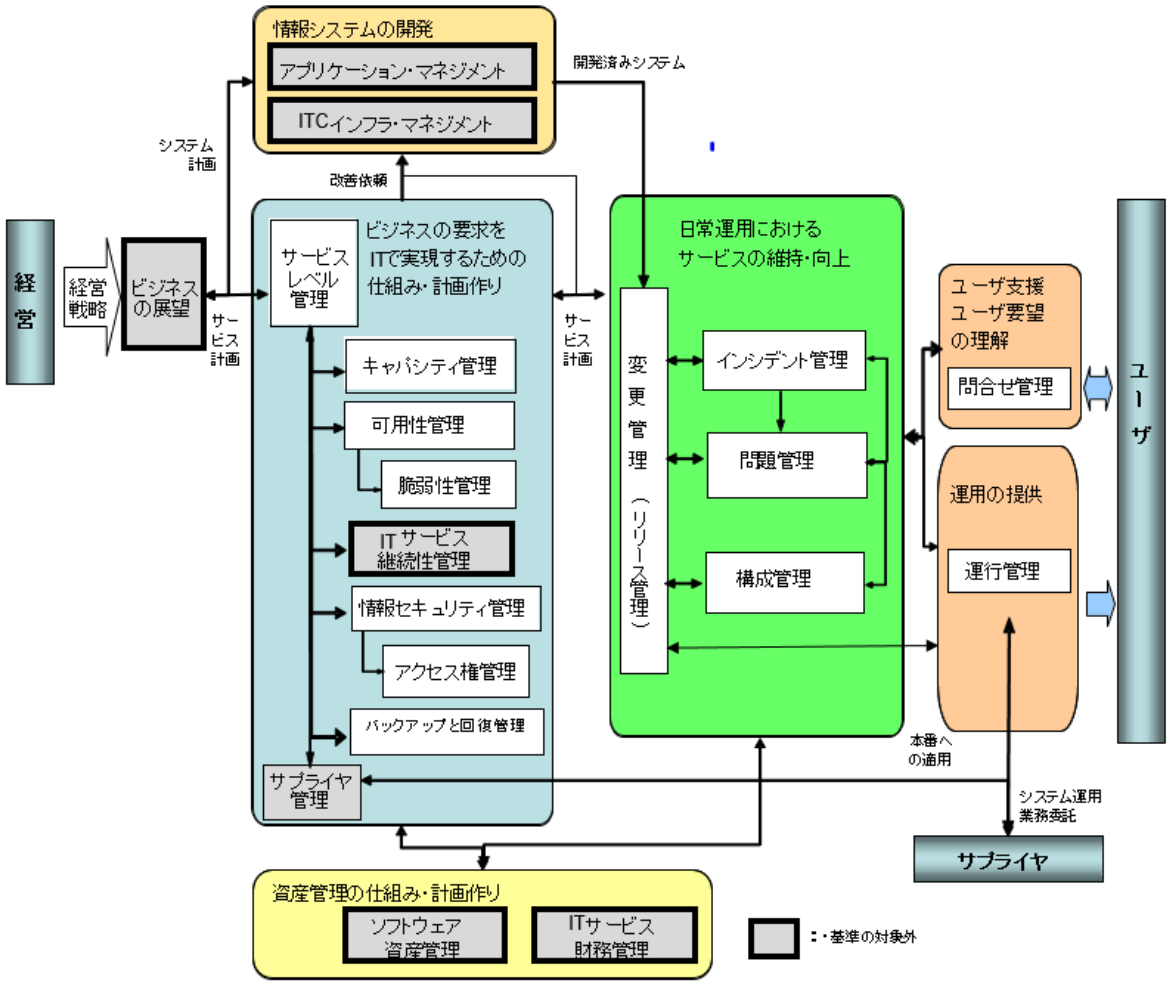
2. システム運用管理業務の概要

PMDA においては情報システムの運用保守を外部委託している状況を踏まえ、運用管理に必要なプロセスのあるべき姿から主要なプロセスを運用管理業務として選定し、以下の13の管理業務について、明確化・標準化を行う。

管理業務	概要
問合せ管理 （サービスデスク）	システムの利用者からの問合せ窓口として、利用者からの各種問合せについて一括受付することにより 問合せに対する早期回答、障害対応への早期エスカレーションを図るとともに、ユーザからの要望を適切に吸い上げる。
インシデント管理	問い合わせに含まれるインシデント、あるいはハードウェア、アプリケーションなどからのインシデント発生の警告／報告を受け、サービスの中断を最小限に抑えながら、可能な限り迅速に通常サービスを回復するよう努める。
問題管理 （再発防止策）	障害（インシデント）の根本的な原因となっている不具合が、ビジネスに与える悪影響を最小化するため、問題を分析し抜本的解決策や回避策を立案する。
変更管理 （課題管理）	情報システムに対する変更の許可と実装を確実に行うための管理をいう。本番環境に対する変更要求を適正な基準で評価・承認を行い、標準化された変更方法、手順が実施されることを確実にする。 また、変更による影響とリスクを最小化し、障害を未然に防止することで、サービス品質の維持・向上に努める。 なお、本基準においては、変更要求の必要性、効果、リスクなど変更の妥当性の評価と承認（変更管理）に加えて、本番環境に対してどのような準備・実行・見直しを行って変更を加えるかの決定（リリース管理）を含めるものとする。
構成管理	情報システムを構成する物理資源・論理資源とその環境を常に把握するための管理をいう。運用・保守業務やそのサービスに含まれる全てのIT資産や構成を明確にし、正確な構成情報と関連文書を提供することで、他のサービスマネジメント・プロセス（インシデント管理、問題管理、変更管理、情報セキュリティ管理等）に信頼できる管理基盤を提供する。
運行管理 （稼動管理）	情報システム全体を予定通り安定的に稼動させるために、システムのスケジュール、稼働監視、オペレーションなど一連の運行を管理する。 ・スケジュール管理 ・オペレーション管理（定型業務、非定型業務） ・稼動監視　・障害対応　・ジョブ運用　・媒体管理 ・本番システム導入・移行時の支援　等

管理業務	概要
バックアップと 回復管理	必要なバックアップを定期的に取得、管理し、障害が発生した場合は、速やかな回復ができるよう、回復要件に基づき必要な回復手順、仕組みを計画、作成、維持する。
情報セキュリティ管理	情報セキュリティポリシーに規定されたセキュリティ対策を実施するために必要な管理要件に基づき、情報セキュリティ管理基準・手順等を作成し、情報セキュリティ管理を行う。
脆弱性管理	情報システムのソフトウェアおよびアプリケーションにおける脆弱性を特定、評価、解消するための管理業務を行う。システム構成を把握した上で、構成要素ごとに関連する脆弱性情報をいち早く「収集」し、影響範囲の特定とリスクの分析によって適用の緊急性と対応要否を「判断」し、判断結果をもとに迅速に「対応」を行う。
アクセス権管理	アクセス方針を定め、アクセス制御の仕組みを構築・維持し、システム・アカウントの申請受付け・登録・変更・削除など管理業務を行う。 ・アプリケーション・システムのアカウント ・サーバのOSアカウント ・DBMSアカウント ・運用支援システムのアカウント ・各種特権アカウント　等
キャパシティ管理	サービス提供に必要となるシステム資源の利用状況の測定・監視を実施し、現在の業務要求（既存の提供サービス量）と将来の業務要求（要求される提供サービス量）とを把握した上で、システム資源がコスト効率よく供給されるように調整・改善策の立案を行う。
可用性管理	ITインフラストラクチャーを整備し、それをサポートするITサービス部門の能力を最適化させることで、ビジネス部門に対して、費用対効果が高いITサービスを持続して提供する。 可用性管理の活動は、既存のITサービスの可用性を日常的に監視・管理する「リアクティブ」なプロセスと、リスク分析や可用性計画の策定や可用性設計基準などの作成を行う「プロアクティブ」なプロセスに分けられる。
サービスレベル管理	「サービスレベル合意書」で定める各種サービスレベル値の達成、維持作業として、管理項目に対する実績データの収集、分析、評価、及び改善策を策定する。 また、運用管理業務における報告データを収集、管理し、月次にユーザへの報告を実施する。

【参考】システム運用管理業務の全体像

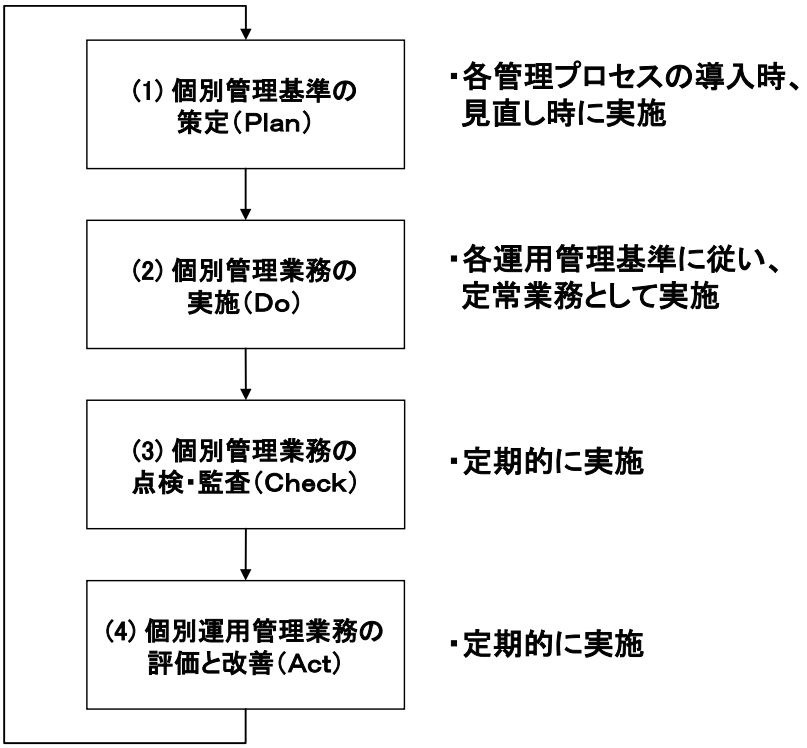


3. 運用管理業務の基本プロセス

（運用管理業務プロセスのPDCAマネジメントサイクル）

他のマネジメント・システムと同様に、運用管理業務プロセスも手順書等を策定して終わりではなく、実際に手順書等に準拠した運用を実施し、定期的に又はシステムの変更やメンバーの入れ替わりなどに合わせて都度、管理プロセスを見直し、必要に応じて改善・是正を行う必要がある。

そのために、運用管理業務プロセスに、個別管理基準の「策定（Plan）」、「実施（Do）」、「点検・監査（Check）」、「評価と改善（Act）」の４つの基本プロセスからなるPDCAマネジメントサイクルを導入し、継続的改善を実施することが重要である。



各基本プロセスの概要は、以下のとおりである。

（1） 個別管理基準の策定 （Plan）
各運用管理業務の実施方針、実施範囲、管理プロセス、業務の管理指標等を含めた管理基準書ならびに管理手順を定める。

（2） 個別管理業務の実施 （Do）
各運用管理業務の実作業を行うとともに、業務遂行に必要な関連情報の蓄積、実績情報の収集保管、およびに評価指標の実績測定を行う。

（3） 個別管理業務の点検・監査 （Check）
各運用管理業務に対し、個別運用管理基準に遵守した運用がなされているか定期的に点検・監査を行い、その結果を分析･評価する。

（4） 個別運用管理業務の評価と改善 （Act）
各運用管理業務に対する評価指標に対する実績管理を行うと共に、品質向上に向けた改善計画を立案し、改善実施を行う。

4. システム運用管理業務の明確化・標準化

4. 1 問合せ管理

(1) 目的

ユーザ及び各業務プロセスオーナからの問合せや依頼に対する受付窓口を一元化することで、各業務の利用ユーザの業務効率性を向上させる。

(2) 業務の概要

問合せ対応では、問合せの受付、クローズ、一次回答、管理プロセスの評価・改善の一連のプロセスを実施する。

(3) 管理対象

本番システム環境で稼動している全てのシステムに係る以下の問合せについて対応する。

- アプリケーション仕様、操作、機能、内容に関する問合せ
- ハードウェア／ソフトウェアに関する問合せ
- 要望
- アプリケーション修繕に対する依頼
- その他の依頼作業

(4) 業務の管理指標＆標準化

問合せ対応業務を評価するための評価指標として以下を定義し、定期的(月次)報告を行う。

①問合せ発生件数（日次集計・月次集計を含む）

②問合せ区分別件数

③問合せ一次回答期限遵守率

④問合せ完了率（一定期間経過後(10 営業日経過後)の完了率）

※報告内容は、各システムの状況に応じて変更しても構わない。

【補足】

問合せにより「システム障害」「セキュリティインシデント」が発覚した場合は、該当問合せは一次回答にてクローズとし、その後は「インシデント管理」にて対応する。

問合せにより「変更」実施が必要となった場合は、対応予定日を回答することでクローズとし、その後は「変更管理（課題管理）」にて対応する。

４．２ インシデント管理

(1) 目的

インシデント管理は、ユーザからの問合せ・連絡、あるいはオペレータや監視システム等によるインシデントの検知を受け、ITサービスの中断を最小限に抑えながら、可能な限り迅速に正常なサービスを回復することを目的とする。

(2) 業務の概要

①インシデントの定義

インシデントとは、ユーザや監視システム等の検知により判明したハードウェアやソフトウェアに関する一般的な障害（システム・ダウン、バグによるアプリケーションの機能停止等）だけでなく、ユーザが日常の操作手順によってITサービスを利用する上で支障がある事象は全てインシデントに包含される。

【注】このインシデントには、情報セキュリティインシデント（不正アクセス・マルウェア検知等）を含む。

また、まだITサービスに影響を与えていない構成アイテムの障害もインシデントとして扱う。

例えば、(i) 二重化されたデータベース・システムの一方がダウンした場合で、まだサービス自体が正常に稼働している場合、(ii) 本番環境のバックアップを検証環境にリストアできない場合、これらをインシデントとして扱う。

②インシデント管理の主な活動

インシデント管理は、インシデントの 4 つのライフサイクル（発見－判別－回復－解決）の内、発見－判別－回復（解決）までをカバーする。（再発防止については、次節の「問題管理」で扱う。）

インシデント管理のプロセスでは、主に次の活動を実施する。

- ・インシデントの検知
- ・インシデントの記録
- ・インシデントの通知
- ・インシデントの分類
- ・インシデントの優先度付け
- ・インシデントの初期診断
- ・エスカレーション
- ・インシデントの調査と診断
- ・復旧(解決)策の実施
- ・インシデントのクローズ

(3) 管理対象

本番システム環境で稼動している全てのシステムのインシデントを管理対象とする。

(4) 業務の管理指標

インシデント管理の管理業務を評価するための評価指標として以下を定義し、定期的(月次)報告を行う。

① 当月インシデント発生件数（総件数、障害ランク別・原因別・システム別件数・解決責任部門別）

② 優先度又は緊急度毎に分類されたインシデントの解決までに要した時間（平均時間）
③ ステータス（記録済み、対応中、クローズ済み等）毎のインシデントの内訳
④ 長期間（発生から１カ月以上）未解決のインシデントの件数と理由および業務影響
⑤ 新規に発生したインシデントの件数とその傾向
⑥ ユーザのトレーニングなど、ITテクノロジーに関連しないで解決されたインシデントの件数
⑦ 解決に要したコスト
⑧ インシデント発生件数の削減率（対前年比）

(5) 標準化

インシデント管理は、PMDA 標準書式を適用する。

①インシデント発生(判明)時

インシデントごとに個票を起票する。この個票は「PMDA 標準書式」を使用する。

※添付「インシデント報告書（ひな型）」を使用する。また「インシデント一覧記載要領」を参照し、対応すること。

※各情報システムの状況等によって、一部改修して使用しても構わない。ただし、必須項目の変更・削除は認めない。

②定期的(月次)報告時

インシデントごとの個票を集計表に転記のうえ報告する。この集計表は「PMDA 標準書式」を使用する。

※添付「インシデント一覧」を使用する。

４．３ 問題管理（再発防止策）

(1) 目的

サービスの信頼性を維持・向上するためには、システムの利用・運用上発生した問題（障害を引き起こす根本的な原因）を確実に解決し、同一障害・類似障害の再発防止のための是正を実施することを目的とする。

(2) 業務の概要

本番サービスに影響を与えた障害を分析し、それらの共通の根本原因を取り除く是正策を実施するまでの一連のプロセスを管理する。 問題管理(再発防止)では、以下を実施する。

- ・問題の傾向分析と課題点の抽出
- ・是正策の検討
- ・是正策の実施

(3) 管理対象

本番システム環境で稼動している全てのシステムの問題を管理対象とする。

(4) 業務の管理指標＆標準化

問題管理(再発防止)業務を評価するための評価指標として以下を定義し、定期的(月次)報告を行う。

① 再発防止策が策定された問題件数（総件数、障害ランク別・原因別・システム別件数・解決責任部門別）
② ステータス（記録済み、対応中、クローズ済み等）毎の再発防止策の内訳
③ 再発防止に要したコスト
④ 長期間（策定から１カ月以上）未実施の再発防止策件数と理由
⑤ 再発防止の実施率（対前年比）

※報告内容は、各システムの状況に応じて変更しても構わない。

４．４ 変更管理

(1) 目的

サービスの信頼性を維持・向上するためには、システムに対する変更について、その妥当性を検証し、変更によるユーザへの影響を最小限にすることが重要である。 変更管理プロセスは、システムに対する変更を一元的に管理することを目的とする。

(2) 業務の概要

変更管理では、変更の申請から変更内容の審査、変更の承認または却下、変更の実施、変更実施結果の報告までの一連のプロセスを管理する。

緊急の場合、対応を優先し所定のプロセスを適宜省略することを可能とするが、事後的に対応できるものについては、事後速やかに対応することとする。

(3) 管理対象

システム運用者（委託先）が運用し本番サービスを提供するシステムの全て又はその一部に対して影響を与える全ての変更を管理対象とする。

本番環境	構成要素（主な要素）
ハードウェア	CPU、DASD・DISK、サーバ、ワークステーション、周辺装置
システム・ソフトウェア	OS、サブシステム、サーバ及びワークステーション OS
ミドルウェア	DBMS、ネットワーク OS
アプリケーション・ソフトウェア	ソース、モジュール、シェル、JCL
ネットワーク・ハードウェア	スイッチ、ルータ、ブリッジ
ネットワーク・サービス	基幹ネットワーク、LAN、インターネット　等
データ	データベース及びファイル内のデータ（に対する直接修正）

(4) 業務の管理指標

変更管理業務を評価するための評価指標として以下を定義する。

① 変更実施件数（総件数、領域別・原因別・システム別件数・解決責任部門別）
② 変更の実装が失敗した件数
③ 変更のバックログの件数
④ 予定期間でクローズされなかった変更の件数
⑤ 変更が原因で発生した変更の件数
⑥ 緊急の変更の件数

(5) 標準化

変更管理は、PMDA 標準書式を適用する。

①変更案件発生時

課題管理表に記入し、変更管理のステイタス（未着手（対応予定日記入）～着手(対応中)～完了）を管理する。

※課題管理表の書式は、各情報システムの任意とする。

②変更実施着手時

変更の着手ごとに個票を起票する。この個票は「PMDA 標準書式」を使用する。

※添付「変更作業申請書（ひな型）」を使用する。

※各情報システムの状況等によって、一部改修して使用しても構わない。ただし、PMDA 側の確

認･承認欄の削除は認めない。

※個票は、「単純な定常作業」に関しては使用しなくても良い。

- 「単純な定常作業」は、各システムにて定義する。
- ただし、定期的（月次）報告には、記載する。

※個票は委託先にて保管し、監査等にて提示要求があった場合は、速やかに提示できるよう対応する

③定期的(月次)報告時

変更実施ごとの個票を集計表に転記のうえ報告する。この集計表は「PMDA 標準書式」を使用する。

※添付「変更作業一覧」を使用する。また「変更作業一覧記載要領」を参照し、対応すること。

※「単純な定常作業」に関しては、「変更作業一覧」の「変更申請」欄及び「完了確認」欄に関する内容を記入し、報告する。

４．５ 構成管理

(1) 目的

システムの構成要素（構成情報）を正確に把握し、常に最新状態にあることを保証する事で、他の運用管理プロセス（障害管理や変更管理等）に対して必要な構成情報を提供できるようにする。

(2) 業務の概要

構成管理では、ITサービス開始時より構成情報を一元管理し、他の運用管理プロセスから最新の構成情報を参照可能にする。

本管理プロセスの開始前に、立案した計画に沿って対象とするITサービスやITコンポーネントの範囲、詳細度のポリシーを策定し、開始時のベースラインを把握する。 次に、構成情報の収集と分類を行った上で構成情報を参照可能な状態に維持する。

本管理プロセスの開始後は、変更管理プロセスと連携し、構成情報が常に最新状態として維持されるようにコントロールを行う。 また、定期的に構成情報の点検を行うことにより、課題や問題点を洗い出し、評価・改善を行う。

(3) 管理対象

構成管理が対象とする構成情報は以下の通りとする。

カテゴリー	管理対象の種類
システム運用管理	各種管理プロセス定義書、手順書、依頼書、CI一覧
システム運用	・ハードウェア、ネットワーク・ハードウェアの一覧、構成図 ・ネットワーク・サービス （WAN、インターネット等)の一覧、構成図 ・システム運用各種手順書（障害対応手順書等）
システム保守	・システム・ソフトウェア、ミドルウェアの一覧、構成図 ・アプリケーション・ソフトウェア(ライブラリ、データ、環境設定情報)
ハウジング	環境設備 （空調設備、電源設備、配線室、配線、管理室)の一覧、構成図
アプリケーション保守	・設計ドキュメント、プログラムソース ・アプリケーション保守用各種手順書（定型作業手順書等）

(4) 業務の管理指標

構成管理業務を評価するための評価指標として以下を定義する。

① 承認されていない構成の件数
② 不正確な構成情報が原因で失敗した変更及び発生した障害の件数
③ CI（管理対象の項目数）の正確さ率
・構成アイテムの管理情報と実態（H/W、S/W、M/W、機器）との整合性の確認

(5) 標準化

○PMDA では、「システム資産簿」を作成してシステムのインベントリ情報を一元管理している。各システムのインベントリ情報を各システムの実装状況を反映した最新状況に更新するとともに、「システム資産簿」を最新の状況に保つため、最新のインベントリ情報を PMDA 標準書式「システム資産簿登録用シート」を使用して、PMDA へ報告する。

４．６ 運行管理

(1) 目的

運行管理の目的は、開発部門より引き継いだ業務アプリケーション・システムを、あらかじめ定められた運行計画に基づき、定められた手順に従ってシステム運用を行うことにより、システム運用の品質の維持・向上を図ることにある。

(2) 業務の概要

運用引継ぎから、システムのスケジュール計画、稼働監視、オペレーションなど一連の運行を管理する。 以下のサブプロセスから構成される。

① 運用引継ぎ
② 運用スケジュールの計画・管理
③ オペレーション実施
④ 稼動監視と障害対応（一次対応）
⑤ セキュリティ監視（対象イベントの検知への対応）
⑥ ジョブ実行管理
⑦ 帳票管理
⑧ 報告管理

(3) 管理対象

本番システム環境で稼動している全ての情報システムの運行を管理対象とする。

(4) 業務の管理指標

運行管理業務を評価するための評価指標として以下を定義する。

① 重要バッチ処理終了時間遵守率
② 重要帳票の配布時間遵守率
③ システムの運行業務に起因した障害の発生件数
・プログラム・JCL等の本番移送のミス、ジョブのスケジュール誤り、操作ミス、監視項目の見落とし／発見遅延、等。
④ 非定型依頼業務の実施件数と正常終了率

(5) 標準化

〇情報システムの運行状況を報告する（月次）（書式任意）

情報システムの稼働状況に加えて、以下の項目の報告を必須とする。

・情報システム及びネットワーク内で発生するイベント（事象）の記録である「ログ」の取得・保存のプロセスの状況を監視し、報告する。
・情報システムの稼働により発生する各種検知メッセージへの対処を記録し、報告する。

４．７　バックアップと回復管理

(1)　目的

障害発生時等において、速やかに正確な回復処置が行えるようにバックアップの取得・リストアの手順を明確にし、安定したサービスの提供を図る。

(2)　業務の概要

アプリケーションオーナーとのサービスレベルまたは管理目標の合意に基づき、システムの回復要件（＊）に見合ったバックアップ・リストア方針を定め、バックアップ対象の選定、手順の明確化を実施する。

日常運用においては、バックアップ取得、バックアップ媒体の保管を行う。

また、定期的に、バックアップ・リストア実績報告を行い、バックアップ・リストアにおける体制、役割、手順の見直しを図る。

（＊）業務の優先度を勘案して有事の際に稼動させるシステムのサービスレベルを定めて、データのバックアップと復旧方法を決定する。

RLO （Recovery Level Objective）：どの範囲、レベルで業務を継続するか

RTO （Recovery Time Objective）：いつまでにシステムを復旧するか

RPO （Recovery Point Objective）：どの時点にデータが戻るか

(3)　管理対象

本番システム環境で稼動している全てのシステムのバックアップとリストアを管理対象とする。

本基準の適用システムに関するOS、データベース、テーブル類、ユーザデータなどのバックアップ計画、バックアップ取得、バックアップ媒体の保管、リストア実施および定期的な実績報告の手続きを対象とする。

各情報システムを構成するサーバや通信回線装置等については、運用状態を復元するために必要な重要な設計書や設定情報等のバックアップについても適切な場所に保管する。

(4)　バックアップデータの保管方法

要保全情報(完全性2)又は要安定情報（可用性2）である電磁的記録若しくは重要な設計書は、バックアップを取得する。

① データベースやファイルサーバのバックアップは、インターネットに接点を有する情報システムに接続しないディスク装置、テープライブラリ装置等に保存する。

② 一般継続重要業務で使用するシステムについては、大規模災害やテロ等による設備・機器の破損を想定し、情報システムの復元に必要な電磁的記録については LTO 等の可搬記憶媒体による遠隔地保管を行う。

③ バックアップの取得方法、頻度、世代等は各システムの方式設計、運用要件に応じて定める。

(6)　業務の管理指標

バックアップと回復管理業務を評価するための評価指標として以下を定義する。

① 当月で計画された定期バックアップの内、バックアップに失敗した件数と理由。

② 当月実施されたリストア件数と内訳（障害対応、調査目的、帳票再作成・出力等）。

③ 当月実施されたリストアの内、リストアに失敗した件数と理由。

(7) 標準化

〇定期的なバックアップが取得されていることを報告する（月次）（書式任意）

〇PMDA では、「リストアの机上訓練」を定期的に実施することを推奨している。

各情報システムにおいては、必要に応じて定期的な訓練実施を行い、結果報告を行う。

４．８ 情報セキュリティ管理

(1) 目的

情報セキュリティ管理は、「情報セキュリティ対策の運用要件」に定める情報セキュリティ対策の運用要件に則り、情報システムのセキュリティを維持・管理し、情報資産を適切に保護することを目的とする。

(2) 業務の概要

情報セキュリティ管理プロセスは、PMDA のリスク管理活動の一環として、ITサービス及びサービスマネジメント活動における全ての情報のセキュリティを、首尾一貫した方針に基づき効果的に管理する。

具体的には、「情報セキュリティ対策の運用要件」に則って、適切にセキュリティ管理策が導入され、維持されていることを確実にするために、情報セキュリティ管理計画の維持・管理を行う。合わせて、情報セキュリティ対策が適切に運用されているかを定期的に点検するとともに、コンプライアンス等の観点からのシステム監査の実施対応をおこなう。

(3) 管理対象

ITサービス及びサービスマネジメント活動における全ての情報セキュリティの管理を対象とする。

(4) 業務の管理指標

情報セキュリティ管理業務を評価するための評価指標として以下を定義する。

① 情報セキュリティ違反・事件・事故の発生件数とその内容
② 発生した情報セキュリティ違反・事件・事故への対策の実施状況
③ 情報セキュリティ監査（内部・外部）及び自己点検で検出された不適合の件数
④ 前回の情報セキュリティ監査及び自己点検で検出された不適合の是正状況

(5) 標準化

○情報セキュリティ遵守状況の報告

・情報セキュリティを遵守していることを定期的(月次)にて報告する
※報告内容の詳細は後述の【補足説明】を参照

・委託先における自己点検を定期的(年 2 回程度)に実施し、点検結果を報告する。
（点検内容は委託先の任意とするが、各情報システムの運用保守業務に携わる要員等が自らの役割に応じて実施すべき対策事項を実際に実施しているか否かを確認するだけではなく、運用保守のプロジェクト体制全体の情報セキュリティ水準を確認する内容とすること。）

【補足説明】

情報セキュリティ遵守状況の報告は、以下の内容を確認し、報告すること

① 情報の目的外利用の禁止
② 情報セキュリティ対策の実施および管理体制（プロジェクト計画書記載内容の遵守）
※委託先において実施するセキュリティ研修や委託先の情報セキュリティポリシー遵守のため取組み内容を含む
※責任者による情報セキュリティの履行状況の確認を含む

③ 体制変更の場合の速やかな報告
④ 体制に記載された者以外が委託業務にアクセスできない（していない）ことの確認
⑤ ※発生した場合は、すぐに検知でき、報告される
⑥ 要員の所属・専門性（資格や研修実績）・実績および国籍に関する情報提供
※変更があれば、その都度情報提供される。
⑦ 秘密保持契約（誓約書）の提出（要員全員が提出）
※委託業務を離れた者の一定期間の機密遵守を含む
※体制変更があった場合の追加提出も含む
⑧ 情報セキュリティインシデントへの対処方法の明確化され、要員に周知されている
⑨ 再委託がある場合は、上記内容を再委託先においても遵守していることが確認されている

４．９ 脆弱性管理

(1) 目的

サーバ装置、端末及び通信回線装置上で利用するソフトウェア（含むファームウェア）やアプリケーションに関連する脆弱性情報の収集とその影響評価に基づく適切な対策を実施するための標準的管理要件を定め、脆弱性によりもたらされる情報セキュリティの脅威について迅速かつ適切に対処することを目的とする。

(2) 業務の概要

脆弱性管理では、システム構成を把握したうえで、管理対象とするソフトウェアのバージョン等の確認から、脆弱性情報の収集、影響評価と対策の要否判定、脆弱性対策計画の策定、脆弱性対策の実施、結果の確認、対策の実施状況のモニタリングまでの一連のプロセスを管理する。

①管理対象ソフトウェアの把握 （管理すべきソフトウェアを特定）

②管理対象ソフトウェアの脆弱性対策の状況確認

②脆弱性情報の収集と識別（当該脆弱性が管理対象ソフトウェアに該当するかの確認）

③影響・リスクの評価と対応要否の判断及び記録

④脆弱性対策計画の策定と承認（変更管理手続きに拠る）

⑤脆弱性対策の検証 （検証環境での稼動確認）

⑥脆弱性対策の実施

⑦脆弱性対策の記録・報告

⑧脆弱性対策の実施状況のモニタリングと継続的改善

(3) 管理の対象

本番システム環境で稼動しているサーバ装置、端末及び通信回線装置上で利用するソフトウェアやアプリケーションに関する全ての脆弱性を管理対象とする。

(4) 業務の管理指標

脆弱性管理業務を評価するための評価指標として以下を定義する。

① 管理対象プロダクツ、バージョンに該当する脆弱性情報件数（通常／緊急）
② 脆弱性対策の評価件数（対策要、対策不要）
③ 対策計画の策定・実施状況（セキュリティパッチ適用、またはその代替策）／予定・実績
・定期報告=脆弱性管理の実施報告
・変更管理＝システム変更作業報告（セキュリティパッチ適用状況報告を含む）
④ 実施可能な脆弱性対策を実施しなかったことによる情報セキュリティインシデントが 1 件も発生しないこと。

(5) 脆弱性管理の要件

脆弱性対策について、以下の管理を行う。

① 対象プロダクト・バージョンの把握

・各情報システムにおいて管理対象とするプロダクトとバージョンを特定するとともに脆弱性情報の収集及びパッチの取得方法を(事前に)整備する。

② 脆弱性情報の収集及び対策の要否判断

・管理対象のプロダクトに係る脆弱性情報の公開状況を定期的に収集する。

・収集した脆弱性情報をもとに影響・緊急度、対策の必要性、情報システムへ与える影響・リスクを考慮し、対策の要否を判断する。

③ 脆弱性対策計画の策定と実施

・対策が必要と判断した場合は、セキュリティパッチの適用計画、または、その代替策(回避方法)の実施計画を策定する。

・対策が情報システムに与える影響について事前検証を行った上、実施する。
対策が情報システムの構成変更を伴う場合は、「4.4 変更管理」に拠るものとする。

・対策計画の策定及び実施状況の管理

(6) 標準化

① 管理状況については PMDA 標準書式を使用する。

・管理対象とするソフトウェアのプロダクトとバージョンについては、各情報システムの設計書等のソフトウェア関連項目を基に、「脆弱性管理対象ソフトウェア一覧」を使用し管理する。

・管理対象とするソフトウェアの脆弱性の有無、対策の要否、対策の実施概要については、「脆弱性対策管理簿」を使用し管理する。

② 定期的(月次)報告

・各情報システムにおける管理対象とするプロダクト・バージョンについて内容に更新があった際は、「脆弱性管理対象ソフトウェア一覧」を使用し速やかに報告する。

・脆弱性対策の要否及び対策の実施状況について、「脆弱性対策管理簿」を使用し、定時(月次)で報告する。

※「脆弱性対策管理簿」の作成にあたっては「脆弱性対策管理簿記載要領」を参照すること。

参考 脆弱性情報収集時の参考 URL 一覧 (「IPA 脆弱性対策の効果的な進め方(実践編)」より)

種別	URL
脆弱性関連情報データベース	■国内 ・JVN (Japan Vulnerability Notes) https://jvn.jp/ ・脆弱性対策情報データベース JVN iPedia https://jvndb.jvn.jp/ ■海外 ・NVD(National Vulnerability Database) https://nvd.nist.gov/ ・Vulnerability Notes Database

	https://www.kb.cert.org/vuls/ ・Metasploit（攻撃情報あり） https://www.metasploit.com/ ・Exploit Database（攻撃情報あり） https://www.exploit-db.com/
ニュースサイト	■国内 ・CNET ニュース：セキュリティ https://japan.cnet.com/news/sec/ ・ITmedia エンタープライズ セキュリティ http://www.itmedia.co.jp/enterprise/subtop/security/index.html ・ITpro セキュリティ https://tech.nikkeibp.co.jp/genre/security/ ■海外 ・ComputerWorld Security （米国中心） https://www.computerworld.com/category/security/ ・The Register Security （英国・欧州中心） https://www.theregister.co.uk/security/
注意喚起サイト	■国内 ・IPA：重要なセキュリティ情報一覧 https://www.ipa.go.jp/security/announce/alert.html ・JPCERT/CC 注意喚起 https://www.jpcert.or.jp/at/2018.html
	・警察庁：警察庁セキュリティポータルサイト https://www.npa.go.jp/cyberpolice/ ■海外 ・米国：US-CERT https://www.us-cert.gov/ncas ・米国：ICS-CERT https://ics-cert.us-cert.gov/
製品ベンダー	■定例アップデート ・マイクロソフト セキュリティ更新プログラム ガイド https://portal.msrc.microsoft.com/ja-jp/security-guidance ・オラクル Critical Patch Update と Security Alerts https://www.oracle.com/technetwork/jp/topics/security/alerts-082677-ja.html

	■クライアント製品など ・Apple セキュリティアップデート https://support.apple.com/ja-jp/HT201222 ・Adobe セキュリティ速報およびセキュリティ情報 https://helpx.adobe.com/jp/security.html ・Mozilla サポートの検索 https://support.mozilla.org/ja/
	■サーバ、ネットワーク製品など ・シスコ - セキュリティアドバイザリ https://www.cisco.com/c/ja_jp/support/docs/csa/psirt-index.html ・HP - サポートホーム https://support.hp.com/jp-ja ・日立 -セキュリティ情報 https://www.hitachi.co.jp/hirt/security/index.html ・富士通 - セキュリティ情報 https://www.fujitsu.com/jp/support/security/ https://www.fujitsu.com/jp/products/software/resources/condition/security/ ・NEC - NEC 製品セキュリティ情報 https://jpn.nec.com/security-info/ ・IBM - IBM Support https://www.ibm.com/support/home/?lnk=ushpv18hcwh1&lnk2=support ・Red Hat - Red Hat Product Errata https://access.redhat.com/errata/#/
	■セキュリティ製品など ・シマンテック -セキュリティアップデート https://www.symantec.com/ja/jp/security_response/securityupdates/list.jsp?fid=security_advisory
	■オープンソースなど ・Apache Foundation https://httpd.apache.org/ (Apache HTTP サーバ) https://tomcat.apache.org/ (Apache Tomcat) https://struts.apache.org/ (Apache Struts) ・ISC (Internet Systems Consortium) https://www.isc.org/downloads/bind/ (BIND) https://www.isc.org/downloads/dhcp/ (DHCP) ・OpenSSL https://www.openssl.org/

4．10 アクセス権管理

(1) 目的

システムを利用するユーザ・アカウントを保護するため、及び、なりすましによる不正ログインの可能性を低減するために、ユーザ・アカウントを役割権限別に分類した上で管理方法を取決めてセキュリティレベルを維持する。

(2) 業務の概要

システムを利用するサーバ OS、ミドルウェア、アプリケーション・ソフトウェア、及びネットワーク機器のアカウントを対象にアクセス権の管理を行う。

(3) 管理対象

本番システム環境での全てのアカウント（社外の取引先等に提供しているアカウントを含む）のアクセス権を管理対象とする。

本番環境	アクセス権管理の対象
システム・ソフトウェア	OS ユーザID
ミドルウェア	DBMSユーザID、ジョブスケジューラ・ユーザID、他
アプリケーション・ソフトウェア	アプリケーション・ユーザID
ネットワーク機器	各ネットワーク機器の管理者用ID

(4) 業務の管理指標

アクセス権管理業務を評価するための評価指標として以下を定義する。

① 期間内に発生したユーザID登録・変更・削除の件数
② 特権（高権限）ユーザID別の貸出し件数と用途
③ アカウントおよびアクセス権の定期棚卸しで、発見された不備項目
④ 不適切／不正なアクセス権限の設定によって発生したインシデントの件数
⑤ アクセス権限の再設定が必要となったインシデントの件数
⑥ 間違ったアクセス権限の設定によって提供不能になったサービスの件数
⑦ 間違ったアクセス権限の設定によって生じた不正アクセスの件数

(5) アカウント管理の要件

・【アカウント（ID）の付与】

①情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む）する。

②識別コードの付与に当たっては、.単一の情報システムにおいて、ある主体に付与した識別コードを別の主体に対して付与することを禁止する

③主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布する。

④識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報を速やかに変更するよう、促す。

⑤知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう主体に注意を促す。

⑥情報システムを利用する主体ごとに識別コードを個別に付与する。ただし、判断の下やむ

を得ず共用識別コード（共有 ID）を付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関するルールを定め、そのルールに従って利用者に付与する。

⑤主体認証情報の不正な利用を防止するために、主体が情報システムを利用する必要がなくなった場合には、当該主体の識別コードを無効にする。

・【特権 ID と使用者の限定】

①使用者限定の保証

・パスワードの堅牢性

できだけ長い桁数、推測困難かつ記憶が容易となる工夫

・パスワードの厳正管理

業務で使用する必要がある者しか知ることができないようにする

パスワード情報へのアクセス制限

ID 使用者の離任時はパスワード変更を必須

②利用時の承認と記録

・特権 ID を利用して作業を行った結果の記録 （特権 ID 使用管理簿の記載）

・利用状況のモニタリング

サーバのログイン・ログアウトログの出力リストと特権 ID 使用管理簿の作業実績に記載されている日時を照合し、記載されている日時から逸脱する時間帯のログデータがないことをチェック

※工数の許す範囲で、重要サーバに絞り、無作為に抽出した数件のログインに該当する作業のチェック等工夫する

(6) 標準化

・全てのアカウント（ID）について、以下の管理を行う。

①アカウント（ID）管理台帳の作成

ID管理台帳を基に ID の新規・変更・削減の状況について、定期(月次)報告する。

②定期(月次)報告

ID管理台帳を基に ID の新規・変更・削減の状況について、定期(月次)報告する。

③ID棚卸し

全てのIDの棚卸しを以下の手順を参考にし、定期的（最低1回／年）に実施し、報告を行う。

（棚卸し手順）

a. 登録 ID 抽出リスト出力
b. ID 管理台帳突合
c. 棚卸しリスト作成
d. ID 使用者の確認、権限の妥当性の検証
e. 不要 ID(初期登録（ビルドイン）ID を含む）削除と不適切権限の修正
f. ID 管理台帳更新
g. 棚卸実施報告書の作成

※アカウント（ID）管理用資料は、「参考資料_ID 管理用各書式ひな型」を参考に各情報システムにおいて適宜定める。

・特権IDについて、以下の管理を行う。

①特権ID台帳の作成

※添付「特権ID管理台帳」を使用する。

※各情報システムの状況等によって、一部改修して使用しても構わない。
ただし、項目の削除は認めない。

※監査等にて提示要求があった場合は、速やかに提示できるよう保管する

②特権ID(システムID)使用管理簿の作成(またはログ抽出)

※添付「特権 ID 使用管理簿」を使用する。各情報システムの状況等によって、一部改修して使用しても構わない。ただし、項目の削除は認めない。

※ログイン・ログアウトのログ(または画面コピー)を必ず保管(または添付)し、監査等にて提示要求があった場合は、速やかに提示できるよう保管する

③定期(月次)報告

特権ID(システムID)台帳ならびに特権ID(システムID)使用状況を、定期(月次)報告する。
(ログまたは画面コピーは、月次報告不要)

④特権ID棚卸し

特権IDの棚卸しを定期的(年 2 回程度)に実施し、報告を行う。(報告書式任意)

棚卸し点検内容は以下の通り

〇台帳は、本当に使用する者を登録しているか?(体制図と一致しているか?)
・体制から外れた者が削除されずに残っていないか?
・使用予定がない者が登録されていないか?

〇台帳と使用管理簿の相関は一致しているか?

〇使用管理簿とログ(または画面コピー)保管の相関は一致しているか?

4. 11 キャパシティ管理

(1) 目的

キャパシティ管理の目的は、ビジネスが必要とするときに、必要なキャパシティを適正なコストで提供することである。 すなわち、

① ビジネスの需要に対する供給
ビジネスの変化に合わせて、ITサービスの対応にもスピードが要求される。 キャパシティ管理は、現在から将来にわたるビジネス需要・要件に合わせて、ITインフラストラクチャーのキャパシティを最大限に活用できるようにすることを目的とする。

② キャパシティに対するコスト
一方、必要以上のキャパシティを確保すると購入や運用のための費用が膨らみ、ビジネスの観点からコストを正当化できない。 キャパシティを最適化し、費用対効果が高いITサービスを提供することもキャパシティ管理の目的である

(2) 業務の概要

このプロセスは、次の3つのサブプロセスから構成される。

① ビジネスキャパシティ管理

ITサービスに対する将来のビジネス需要・要件を収集・検討し、それによって、ITサービスのキャパシティを確実に実装させるための計画の立案、予算化、構築がタイムリーに実施されるようにする。

② サービスキャパシティ管理

実際のサービスの利用と稼働のパターン、山と谷を理解して、運用中のITサービスのパフォーマンスを監視し、それによって、SLAの目標値を達成し、ITサービスを要求どおりに機能させる。

③ コンポーネントキャパシティ管理

ITインフラストラクチャーの個々のコンポーネントのパフォーマンスとキャパシティ、使用状況を監視し、それによって、SLAの目標値を達成・維持するために、コンポーネントの利用を最適化する。

(3) 管理対象

本基準の適用システムにおけるハードウェア、ソフトウェア、ネットワーク、アプリケーション、及び人的リソースを対象とする。

(4) 業務の管理指標

キャパシティ管理業務を評価するための評価指標として以下を定義する。

① CPU、ディスク、メモリ、ネットワーク容量などの閾値に対する需要の割合
② ITサービスのパフォーマンス不足に起因するSLA違反やインシデントの発生件数
③ ITコンポーネントのパフォーマンス不足に起因するSLA違反やインシデントの発生件数
④ 正規の購入計画に含まれていなかった、パフォーマンスの問題解決のために急きょ行った購入の数又は金額

4．12 可用性管理

(1) 目的

可用性管理の目的は、ビジネス部門に対して、費用対効果が高いITサービスを持続して提供することであり、そのためにITインフラストラクチャーを整備し、それをサポートするITサービス部門の能力を最適化させる。

(2) 業務の概要

可用性管理の活動は大きく、1）可用性要件の把握、2）可用性の設計、及び3）可用性の改善活動の3つに分けられる。

具体的には、以下の可用性管理の3要素の目標値を設定し、設定した可用性のレベルを達成・維持・向上させることである。

① 可用性

可用性とは、ITサービスが必要なときに使用できる割合のことで、一般的には稼働率という指標を用いて表される。

稼働率（%）＝（サービス提供時間－停止時間）÷サービス提供時間

② 信頼性

提供されるITサービスにおける、不具合の発生しにくさ／故障しずらさを表す。
平均故障間隔＝（使用可能な時間－総停止時間）÷（サービス中断の回数－1）

③ 保守性

ITサービスが停止又は品質低下した際に、いかに早く復旧できるかを示す指標。
平均修理時間＝修理時間の合計÷サービス中断の回数

可用性について極めて重要なことは、ユーザの求めるシステムの可用性レベルをどのように達成するかについて、システム設計時に真剣に検討し、システム構築時に実現し、システムの運用において継続的に改善することである。

(3) 管理対象

本基準の適用システムにおけるハードウェア、ソフトウェア、ネットワーク、及びアプリケーションを対象とする。

(4) 業務の管理指標

可用性管理業務を評価するための評価指標として以下を定義する。

① 可用性の割合
② 平均故障間隔
③ 平均修理時間
④ サービスの中断回数
⑤ 定期的なリスク分析、及びレビューの完了の件数

4．13　サービスレベル管理

(1)　目的

ユーザニーズを満足する適正なサービスレベルおよび管理指標を設定し、これを実績管理することにより質の高いサービスの提供を図る。

(2)　業務の概要

サービスレベルおよび各個別管理業務での管理指標の実績データを定期的に把握し、サービスレベル指標と実績の差異や傾向を継続的に分析することにより、改善策を立案し実施する。

(3)　管理対象

IT 部門が提供する全ての IT サービスに関するサービスレベルおよび各個別管理業務での管理指標を管理対象とする。

(4)　業務の管理指標

サービスレベル管理業務を評価するための評価指標として以下を定義する。

①「サービスレベル合意書」の各サービスレベル項目の達成率

②各個別管理業務での管理指標の達成率

(5)　標準化

サービスレベル管理業務を定期的(月次)に報告する。

①「サービスレベル合意書」の各サービスレベル項目の達成率

②各個別管理業務での管理指標の達成率

以上

別紙13 情報セキュリティ対策の運用要件

情報システムの運用・保守の業務遂行にあたっては、調達・構築時に決定した情報セキュリティ要件が適切に運用されるように、人的な運用体制を整備するとともに、機器等のパラメータが正しく設定されていることの定期的な確認、運用・保守に係る作業記録の管理等を確実に実施すること。

対策区分	対策方針	対策要件	運用要件	定期点検
侵害対策 （AT：Attack）	通信回線対策 （AT-1）	通信経路の分離 （AT-1-1）	不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離すること。ネットワーク構成情報と実際の設定を照合し、所定の要件通りに設定されていることを定期的に確認すること。	セキュリティヘルスチェック（構成管理資料の原本と実際の設定状況を目視にて突合せチェックすることにより各種セキュリティ設定の不正変更の有無をチェックする）と合わせて実施し報告すること。
		不正通信の遮断 （AT-1-2）	通信に不正プログラムが含まれていることを検知したときに、その通信をネットワークから遮断すること。	
		通信のなりすまし防止　（AT-1-3）	通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能について、有効に機能していることを定期的に確認すること。	セキュリティヘルスチェック（構成管理資料の原本と実際の設定状況を目視にて突合せチェックすることにより各種セキュリティ設定の不正変更の有無をチェックする）と合わせて実施し報告すること。
		サービス不能化の防止　（AT-1-4）	サービス不能攻撃を受けているかを監視できるよう、稼動中か否かの状態把握や、システムの構成要素に対する負荷を定量的(CPU 使用率、プロセス数、ディスク I/O 量、ネットワークトラフィック量等)に把握すること。監視方法はシステムの特性に応じて適切な方法を選択すること。	
	不正プログラム対策 （AT-2）	不正プログラムの感染防止　（AT-2-1）	不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。不正プログラム対策ソフトウェア等により定期的に全てのファイルに対して、不正プログラムの検査を実施すること。	
		不正プログラム対策の管理　（AT-2-2）	不正プログラム対策ソフトウェア等の定義ファイルの更新状況を把握し、不正プログラム対策ソフトウェア等が常に有効に機能するよう必要な対処を行うこと。	

	セキュリティホール対策（AT-3）	運用時の脆弱性対策　（AT-3-2）	情報システムを構成するソフトウェア及びハードウェアのバージョン等を把握して、製品ベンダや脆弱性情報提供サイト等を通じて脆弱性の有無及び対策の状況を定期的に確認すること。脆弱性情報を確認した場合は情報システムへの影響を考慮した上でセキュリティパッチの適用等必要な対策を実施すること。 対策が適用されるまでの間にセキュリティ侵害が懸念される場合には、当該情報システムの停止やネットワーク環境の見直し等情報セキュリティを確保するための運用面での対策を講ずること。	脆弱性対策の実施状況は、月次で報告すること。
不正監視・追跡 （AU: Audit）	ログ管理（AU-1）	ログの蓄積・管理（AU-1-1）	情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログ（システムへのログオンや資源へのアクセスのロギング等）を取得すること。	ログが所定の要件通り、取得・蓄積されていることを確認すること。（年１回以上）
		ログの保護　（AU-1-2）	取得・蓄積されたログが不正な改ざんや削除が行われないようログの格納ファイルのアクセス権を制限する等必要な対策を講じること。	取得・蓄積されたログが不正な改ざんや削除が行われていなことを確認すること。（年１回以上）
		時刻の正確性確保（AU-1-3）	システム内の機器の時刻同期の状況を確認すること。	
	不正監視（AU-2）	侵入検知　（AU-2-1）	不正行為に迅速に対処するため、通信回線を介して所属するＰＭＤＡ外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知した場合は通信の遮断等必要な対処を行うこと。	
アクセス・利用制限（AC: Access）	主体認証（AC-1）	主体認証　（AC-1-1）	主体認証情報（ＩＤ、パスワード）は不正に読み取りできないよう保護すること。	
	アカウント管理（AC-2）	ライフサイクル管理　（AC-2-1）	主体が用いるアカウント（識別コード、主体認証情報、権限等）は、主体の担当業務に必要な範囲において設定すること。 また、アカウント管理（登録、更新、停止、削除等）の作業内容は記録し、証跡を保管すること。 アカウント棚卸を定期的に実施し、不要なアカウントを削除すること。	アカウント棚卸を定期的（年１回以上）に実施すること。
		アクセス権管理（AC-2-2）	主体が用いるアカウント（識別コード、主体認証情報、権限等）は、主体の担当業務に必要な範囲において設定すること。また、アカウント管理（登録、更新、停止、削除等）の作業内容は記録し、証跡を保管すること。 権限の再検証を定期的に実施し、不要な権限を削除すること。	ユーザーＩＤの棚卸と合わせて実施すること。

		管理者権限の保護（AC-2-3）	システム特権を付与されたアカウント及び使用者を特定し、アカウントの使用状況を記録し、アカウントの不正使用がないことを定常的に確認すること。	管理状況を「特権ＩＤ台帳」及び「特権ＩＤ使用管理簿」により、月次で報告すること。
データ保護（PR: Protect）	機密性・完全性の確保（PR-1）	通信経路上の盗聴防止　（PR-1-1）	通信回線に対する盗聴行為による情報の漏えいを防止するため、通信回線を暗号化する機能について、有効に機能していることを定期的に確認すること。	セキュリティヘルスチェック（各種セキュリティ設定の不正変更の有無、および不正操作の痕跡の有無の確認）と合わせて実施し報告すること。
		保存情報の機密性確保　（PR-1-2）	情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限すること。構成情報と実際の設定を照合し、所定の要件通りに設定されていることを定期的に確認すること。 また、業務データへのアクセス権限の付与状況を点検し、不要なアクセス権限が付与されていないことを確認すること。	ユーザーＩＤの棚卸と合わせて実施すること。
		業務データへのアクセス管理	情報の格付の見直し及び再決定が行われた際や、当該情報システムに係る職員等の異動や職制変更等が生じた際には、情報に対するアクセス制御の設定や職務に応じて与えられている情報システム上の権限が適切に変更されていることを確認すること。	ユーザーＩＤの棚卸と合わせて実施すること。
		受託者によるアクセス	受託者は受託した業務以外の情報へアクセスしないこと。	情報セキュリティ遵守状況は月次で報告すること。
物理対策（PH: Physical）	情報窃取・侵入対策（PH-1）	情報の物理的保護（PH-1-1）	受託者の管理区域において、受託者がＰＭＤＡより提供された情報を格納する機器は、情報の漏えいを防止するため、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。 また受託者の管理区域内のバックアップテープ等の可搬記憶媒体についても、管理（受領、返却、廃棄、等）の内容を台帳に記録し、証跡を保管すること。	情報セキュリティ遵守状況は月次で報告すること。 可搬記憶媒体の棚卸と合わせて実施すること。
		侵入の物理的対策（PH-1-2）	受託者の管理区域において、受託者がＰＭＤＡより提供された情報を格納する機器は、物理的な手段によるセキュリティ侵害に対抗するため、外部からの侵入対策が講じられた場所に設置すること。	情報セキュリティ遵守状況は月次で報告すること。
		入退室管理の履行	ＰＭＤＡが管理するサーバ室、事務室等の管理区域への入退出については、ＰＭＤＡ入退室管理規程を遵守すること。	

			ＰＭＤＡの管理区域内での作業は、原則として、ＰＭＤＡ職員の立会いのもとで行うこと。	
障害対策（事業継続対応）（DA: Damage）	構成管理（DA-1）	システムの構成管理　（DA-1-1）	情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を実際のシステム構成と合致するように維持・管理すること。	変更作業時の構成管理資料の更新については、「変更作業一覧」により、月次で報告すること。
	可用性確保（DA-2）	システムの可用性確保　（DA-2-1） 情報のバックアップの取得	システム及びデータの保全が確実に実施されるため、システム及びデータのバックアップが所定の要件通りに取得されていることを定期的に確認すること。 また、回復手順について机上訓練を実施し、バックアップや回復手順が適切に機能することを確認する。	バックアップの実施状況は、月次で報告すること。 バックアップによるリストア等回復手順については、机上訓練を年１回以上実施すること。
サプライチェーン・リスク対策（SC: Supply Chain）	情報システムの構築等の外部委託における対策（SC-1）	委託先において不正プログラム等が組み込まれることへの対策（SC-1-1）	情報システムの運用保守において、ＰＭＤＡが意図しない変更や機密情報の窃取等が行われないことを保証するため、構成管理・変更管理を適切に実施すること。	変更管理の状況は「変更作業一覧」により、月次で報告すること。